ORDER **1370.78**

AIRWAY FACILITIES
INFORMATION RESOURCES MANAGEMENT

October 28, 1994

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

Distribution: A-W(AF/FZ/LM/NS/OP/OS/SR)-3; A-X(AF)-3; A-FAF-0(LTD) ; AMA-400 **Initiated By: AFZ-500**

RECORD OF CHANGES

DIRECTIVE NO. 1370.78

CHANGE TO BASIC	SUPPLEMENT			OPTIONAL	CHANGE TO BASIC	SUPPLEMENTS			OPTIONAL

FOREWORD

It has become increasingly recognized in Airway Facilities strategy and practice that improved information management is a key requirement for meeting the AF mission. This in turn requires that a clear and consistent set of Information Resources Management (IRM) policies and procedures be defined and implemented throughout AF.

This order is intended to complement and extend FAA Order 1370.52C, Information Resources Management--Policies and Procedures, to meet the specific requirements of the AF information management environment. It will support IRM managers and others in meeting the objectives of the AF IRM program. It addresses IRM planning, procurement, information systems development, data management, network management, and configuration management in the AF environment.

Since everyone in Airway Facilities produces, uses, and/or manages information needed to meet AF mission objectives, implementation of the described policies and procedures will require the active involvement of all management levels of Airway Facilities.

Joaquin Archilla
Associate Administrator for
Airway Facilities

TABLE OF CONTENTS

CHAPTER 1. GENERAL

1-1. PURPOSE.

a. This order implements FAA and other federal Information Resources Management (IRM) policies for Airway Facilities (AF). It prescribes requirements, processes, and procedures for: short-term tactical and long-term strategic IRM planning; procurement of automatic data processing and telecommunications equipment, software, and services; information system development and maintenance; network management; data management; and configuration management. To address specific AF IRM requirements, this order complements and extends FAA Order 1370.52C, Information Resources Management--Policies and Procedures.

b. The order provides a framework for improved management of AF corporate electronic data. Such data includes all information used in the conduct of AF business that is stored or accessed via automated information systems. Additionally, the order describes the roles and responsibilities of the AF senior management, organizations, and program offices involved in various aspects of managing information resources.

1-2. DISTRIBUTION.

This order is distributed to branch level in AF Washington headquarters, regions, centers, field offices and facilities.

1-3. RELATED PUBLICATIONS.

a. DOT H 1350.2, Departmental Information Resources Management Manual (DIRMM).

b. Order DOT 4200.14C, Major Acquisition Policies and Procedures (MAPP).

c. Order DOT 4200.16A, Advance Acquisition Planning and Annual Procurement Plans.

d. Order DOT 1740.1A, Administrative Telephone Service and Equipment.

e. Order DOT 1640.1C, DOT Computer Security Program (COMPUSEC) Manual.

f. Federal Acquisition Regulation (48 CFR).

g. FAA Order 1370.52C, Information Resources Management — Policies and Procedures.

h. FAA Order 1810.1F, Acquisition Policy.

i. FAA Order 6110.5, Computer Aided Engineering Graphics (CAEG).

j. FAA Order 1375.1B, Data Standards.

k. FAA Order 1375.2A, Standard Data Elements and Codes, General Standards.

l. FAA Order 1375.3B, Standard Data Elements and Codes, Airport Standards.

m. FAA Order 1800.8F, National Airspace System Configuration Management.

n. FAA Order 1800.63A, National Airspace System (NAS) Deployment Readiness Review (DRR) Program.

o. FAA Order 1600.54B, FAA Automated Systems Security Handbook.

p. FAA Order 4453.1B, Quality Assurance of Material Procured by FAA.

q. FAA-Standard-021A, Configuration Management (Contractor Requirements).

r. FAA-STD-013, Quality Control Program Requirements.

s. FAA-STD-016, Quality Control System Requirements.

t. FAA-STD-018, Computer Software Quality Program Requirements.

u. FAA-STD-016, Quality Control System Requirements.

v. FAA Telecommunications Strategic Plan, as amended.

w. Future FAA Telecommunications Plan (Fuchsia Book), Telecommunications Management and Operations Division, April 1993;

x. Current FAA Telecommunications Plan (Currant Book), Telecommunications Management and Operations Division, Fiscal Year 1991.

y. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 200, National Policy on Controlled Access Protection.

z. NBS Special Publication 500-149, Guide on Data Entity Naming Conventions.

aa. Government Open Systems Interconnection Profile, FIPS Pub 141.

bb. Data Standards and Guidelines/Representations and Code Set, FIPS PUB 19-2.

Specific related publications are listed in individual chapters.

1-4. DEFINITIONS.

Appendix 8, Definitions, defines terms essential to understanding this order.

1-5. SCOPE OF APPLICATION.

a. Inclusions. This order applies to all:

(1) Automated information systems within AF.

(2) Management requirements for federal information processing (FIP) hardware, software, networks, and telecommunications resources (including facilities and services).

(3) All data and information generated or maintained by AF with the exception of specific exclusions. (See 1-5.c below.)

(4) Peripheral equipment, such as printers and modems, used in conjunction with FIP hardware.

(5) In-house or contracted studies for the development and evaluation of such systems or requirements.

(6) Procurements of FIP and telecommunications equipment and services that require approval.

b. Applicability. This order applies without regard to the manner and source of funding or organizational control over services, and applies to both in-house and contracted services.

c. Exclusions. This order does not apply to systems that directly support the operational activities associated with the real-time Air Traffic Control System. It does, however, apply to non-real-time Air Traffic related information that can be used as a corporate asset for AF.

1-6. APPLICABLE STATUTORY AND REGULATORY REQUIREMENTS.

This order implements policies defined in laws and regulations related to management of information in the Federal government. These include:

a. "Brooks Act", Automatic Data Processing Equipment, Amendment to Title I of the Federal Property and Administrative Services Act 1949 (Public Law 89-306, 40, USC 759)

b. Paperwork Reduction Act (PRA) of 1980, as Amended (Public Law 96-511, 44 USC Chapter 35); and the Paperwork Reduction Reauthorization Act (PRRA) of 1986 (Public Law 99-500 Title VIII).

c. Report of the National Performance Review GPO S/N 040-000-00592-7.

d. OMB Circular A-123 - Internal Control Systems.

e. OMB Circular A-130 - Management of Federal Information Resources.

f. Presidential Executive Order 12352, Federal Procurement Reforms.

g. Federal Information Resources Management Regulation (FIRMR).

1-7. AUTHORITY TO CHANGE THIS ORDER.

The Director of Resources Management is authorized to issue changes to this order with the following exceptions: changes in policy,

delegation of authority, and/or assignment of responsibility. The Associate Administrator issues and approves changes in AF orders, delegation of authority, and assignment of responsibility.

CHAPTER 2.
GENERAL REQUIREMENTS AND RESPONSIBILITIES

SECTION 1. IRM CONCEPTS AND GUIDELINES

2-1. INFORMATION RESOURCES MANAGEMENT PROGRAM CONCEPTS.

The FAA's approach to information resources management features depends on integrated support from many organizations and managers. These include:

a. National program offices that are responsible for the planning, budgeting, implementing, and funding of IRM efforts vertically throughout their respective organizations. "Vertical" in this concept refers to program management and associated organizational functionality from the headquarters level down through corresponding program activities in the regions to the field offices.

b. An AF Information Resources Management (IRM) program to enable vertical planning, budgeting, and implementation of IRM policy throughout AF organizations. Such activities shall be guided by long-term strategic plans and short-term tactical plans regularly reviewed and updated to serve as a basis for IRM management direction.

c. An AF Manager of Information Resources Management who, on behalf of AF-1, executes all IRM-related responsibilities which encompass program management, planning, information systems management, acquisition of information resources, and the development of key corporate information assets, e.g., an Executive Information System for AF management.

d. An IRM Division to coordinate and integrate the efforts of the individual program organizations into an effective and efficient AF-wide IRM program.

e. Designated regional and service information resources management representatives (designated IRM Representatives) who are responsible for identifying and documenting the IRM needs and requirements of their respective offices, services, regions, and centers, and for coordinating all IRM-related activities within their program organization.

f. Regional division managers, sector managers, and program managers who advocate and support a consistent approach and organization structure to support the AF IRM Program.

2-2. AF IRM GUIDING PRINCIPLES.

a. The guidelines and requirements contained in this order support the broad changes in the management of information that have been fostered by efforts such as the National Performance Review and the FAA Corporate Systems Architecture Initiative. These programs undertake to use information technology to provide improved federal services with fewer financial and personnel resources. The means of "achieving more with less" includes simplified and reduced paperwork, improved business processes and results, and increased measurement and accountability.

b. The focus of FAA and federal IRM policies is on the management of information as opposed to management of technology. (See OMB Circular A-130). The concept behind the AF IRM program is to ensure that managers and employees can access information critical to decision-making and business functions from the universe of significant business data. Policies related to the sharing, security, privacy, standards, and access to information are intended to enable improved business processes to meet FAA mission requirements more effectively at less cost. The effective use of information will be promoted by means of appropriate training and development of shared information systems that serve critical business requirements.

c. Development and maintenance of AF systems and data are guided by the following principles:

(1) Priorities for AF IRM investments will be mission-driven, as documented in the AF Strategic Plan. Actions for IRM are determined by the AF IRM Strategic Planning Process, and shall be implemented in support of opportunities to carry out Business Process Improvement.

(3) IRM investments shall be consistent with corporate IRM planning, frameworks and initiatives such as the FAA's Corporate Information Technology Strategic Plan and the FAA Corporate Systems Architecture. AF IRM initiatives shall support these efforts to create consistent approaches, standards, and infrastructure to support corporate management of information.

(4) Strategies and implementation plans for AF IRM will be based on a common standards-based architecture, including computing systems, communications, applications, and data. The common standards will provide the basis for interoperability and interconnectivity.

(5) New technology will be introduced with minimum disruption to the information systems environment.

(6) Equipment dedicated to single applications shall be avoided, unless a dedicated system is required to satisfy a critical functional requirement. Program managers shall seek opportunities, such as client-server implementations, to minimize cost and maximize efficiency through serving multiple applications, purposes, and programs.

(7) AF data will be managed as a corporate asset to be shared among all organizations that have the need and authority to access the data.

(8) A consistent desktop office automation (OA) capability, including connectivity to external information systems, will be provided to all users who have the need.

(9) Training will be provided to AF staff to facilitate effective use of new information technology. Staff will also be trained in new processes and procedures for management of AF corporate information and associated resources to accomplish job responsibilities.

(10) Computer processing requirements will be met in accordance with General Services Administration (GSA), DOT, and FAA regulations and directives.

(11) AF systems development will employ state-of-the-art techniques and approaches aimed at reducing the systems life cycle, including libraries of reusable code, computer-assisted software engineering (CASE) methodologies and tools, and rapid application development (RAD).

2-3. INFORMATION SYSTEMS SUPPORT.

The following principles shall guide the development of services that support the implementation and use of AF information systems within the scope of this order (see paragraph 1-5):

a. Whenever possible, existing commercial off-the-shelf (COTS) software packages that satisfy a user's requirements will be used instead of developing new application software.

b. All user software will be documented, configured, maintained, and managed to reduce reliance upon individuals and/or specific organizations that operate, modify, or enhance the software.

c. Applications will be developed and maintained in a "modular" fashion, i.e., program components should be designed to be reusable and modifiable.

d. Data structures and software modules will be designed to be shared and reused to improve reliability and minimize life-cycle development and maintenance costs.

e. Applications should have a common user interface to reduce errors and training costs.

f. Standard configuration management practices will be applied to general-purpose software in order to control access, modifications, security, maintenance, software version control, release specifications, and libraries.

2-4. STANDARDS.

a. The following goals guide the implementation of AF information system standards:

(1) **Interoperability.** A major objective of FAA information systems architecture is the linkage among mission applications and databases involving safety, air traffic management, security, logistics and maintenance.

(2) **Portability.** Standards for systems and development environments will enable applications to be developed once for implementation in multiple information system environments.

(3) **Improved Data Management and Software Reusability.** Implementation of an information repository (corporate data dictionary/directory) will enable the FAA and AF to standardize and control data definitions and the environment for software development.

(4) **Improved Reliability of Data.** Data standards and reduced duplication of data will improve the accuracy of data used in multiple applications.

(5) **Reduced Costs for Applications Development and Training.** A standard application development environment and a uniform user interface to applications will reduce costs associated with the development, maintenance and use of applications.

(6) **Enhanced Development Processes.** Standard development environments and reusable components will enhance the speed and reliability of software development.

(7) **Enhanced Security.** The standards framework will promote security requirements for applications, databases, and networks.

b. AF shall implement an architecture for information systems that supports the federal Open Systems Environment (OSE). Requirements for open systems are described in FIPS Pub 141, Government Open Systems Interconnection Profile. The OSE consists of a layered set of defined information management services with associated standards for data formats and interfaces. The architecture shall support corresponding FAA, AIT, DOT and other federal requirements, including specified ISO, ANSI, and IEEE standards.

c. The IRM Division shall oversee the definition and monitor the implementation of the standards framework for AF.

d. The designated AF IRM Representatives and Program Managers for major systems are responsible for implementation of AF and higher-level standards and for development of migration plans for their respective areas.

2-5. TRAINING.

a. All practices affecting information systems planning, development, and operations shall be designed to maximize ease of use and meet training requirements throughout the life of the information system.

b. Applications shall be designed to minimize requirements for specialized expertise and experience. This implies that graphical user interfaces and other standards shall be employed to create a uniform and intuitive means by which users interact with information systems.

SECTION 2. ROLES AND RESPONSIBILITIES

2-6. IRM ORGANIZATION.

IRM for AF is supported at the headquarters level by the AF IRM division. Within each region and center, a single AF IRM representative is designated to oversee and coordinate at appropriate levels the implementation of IRM policies, procedures, and initiatives.

2-7. GENERAL ROLES AND RESPONSIBILITIES.

IRM responsibilities for specific organizational levels are described as follows:

a. The Manager of the AF IRM Division is responsible for:

(1) Establishing AF-wide IRM guidelines, requirements, and procedures.

(2) Managing the budget for National Airspace System Management Automation Program (NASMAP) and expenditures related to headquarters IRM and local-area network (LAN) administration.

(3) Developing and updating AF IRM Plans.

(4) Monitoring the implementation of AF IRM Plans.

(5) Performing routine IRM program reviews to ensure compliance to established policies.

(6) Communicating IRM issues to AF senior management, designated IRM Representatives and other AF organizations, as appropriate.

(7) Serving as the AF IRM Representative to external organizations including the Information Resources Management Committee (IRMC) and the Office of Information Technology (AIT).

(8) Ensuring that AF IRM national orders, plans and standards are coordinated with the Office of Information Technology.

(9) Ensuring communication and collaboration with the Office of Information Technology and other information management organizations in the development of an FAA corporate IT infrastructure.

(10) Collecting and integrating AF-wide IRM requirements.

(11) Implementing systems to support corporate information access requirements.

b. Headquarters program directors, regional division managers, and AF managers at the centers are responsible for:

(1) Appointing the designated IRM Representatives (one per region and center) and other IRM staff to implement IRM policies and meet the IRM requirements of the user community.

(2) Implementing FAA IRM policies in the establishment of these positions and of appropriate levels of authority.

(3) Reviewing regional, center, or Service IRM plans and ensuring integration of these plans in all other appropriate plans.

c. Sector Managers are responsible for:

(1) Appointing an IRM Representative and other IRM staff to support the user communities as well as fulfilling the responsibilities of these positions (listed below) in support of overall AF IRM program management.

(2) Following established guidelines in the establishment of these positions and the establishment of appropriate levels of authority.

(3) Reviewing regional, center, or Service IRM plans and ensuring integration of these plans in all other appropriate plans.

d. Designated AF IRM Representatives, representing FAA headquarters, the regions, and centers, serve as focal points for coordinating IRM activities and facilitating the effective use of information resources throughout the AF. While regional IRMs have traditionally supported offices reporting to the regional/center division managers, the designated IRM Representatives must effect proper coordination with the AF IRM Division required by the vertical program concept. They are responsible for:

(1) Providing a single point of contact within their respective organization/program office for all IRM-related activities including acquisition, configuration management, information systems development and maintenance, and policy compliance.

(2) Making appropriate recommendations to division and branch management to meet IRM requirements and objectives, and ensuring that division and branch

managers are kept informed of IRM program initiatives and activities.

(3) Assign resources to support specific IRM programs (e.g. RTP, CAEG, TIMS) within regions.

(4) Representing all AF IRM interests and encouraging the use of sound IRM principles.

(5) Participating in IRM planning activities.

(6) Developing and maintaining strategic plans and providing guidance on tactical plans for all organizational elements they represent.

(7) Serving as liaison between users and upper management.

(8) Establishing strategic IRM directions, goals and objectives for divisions.

(9) Monitoring compliance with all department and agency orders related to IRM.

(10) Implementing components of the AF IRM Program Plan, as appropriate.

(11) Developing and implementing a regional AF IRM order based upon this order, which contains guidelines and policy implementation requirements specific to the region.

(12) Coordinating and integrating IRM requirements with the agency budgetary process and monitoring the financial aspects of information resources activities within assigned program/organizational areas.

(13) Approving the acquisition of hardware, software, and related FIP services within their delegated acquisition review authority.

(14) Ensuring compliance with the Federal Information Resources Management Regulation (FIRMR) for hardware, software, and services-related acquisitions covered by the FIRMR.

(15) Identifying, updating, and tracking IRM projects and activities.

(16) Assisting in conducting project reviews and triennial reviews of individual automated information systems.

(17) Assisting program organizations in identifying program requirements for automated information systems.

(18) Providing guidance to and consulting with the Program Managers in obtaining resources to implement and maintain operations of new information systems.

(19) Providing advice and assistance in designating project managers to conduct and oversee developmental systems work and advice and assistance in designating Information Systems managers for managing on-going systems and operational work assigned to their organization.

(20) Identifying, reviewing, and coordinating applications of local systems which may be useful to other regions, centers, offices, and services and facilitating the sharing of local systems which are in use at more than one office, service, region, or center.

e. Program Managers for Major Systems are responsible for:

(1) Implementing IRM principles, requirements, and procedures in the development and operation of information systems within their areas of responsibility.

(2) Providing for initial and follow-on training in use and operation of information systems.

(3) Managing resources and budgets to achieve program goals and objectives.

(4) Participating in IRM planning, policy development, and implementation.

2-8. ACQUISITION MANAGEMENT ROLES AND RESPONSIBILITIES.

a. The AF IRM Division will review IRM acquisition plans and strategy throughout AF for reasonableness and consistency with established plans.

b. Designated AF IRM Representatives will review all IRM acquisition requests for conformance to standards, regulations, and

other IRM requirements, and also ensure that the request is reviewed at the appropriate levels.

2-9. NETWORK MANAGEMENT ROLES AND RESPONSIBILITIES.

a. Planning and operations of telecommunications services and facilities within the FAA are the responsibility of the National Operations Division (AOP-100); Operations Concepts, Planning, and Performance Division (AOP-200); the Automated Operations Systems Division (AOP-300); the Telecommunications Network Planning and Engineering Division (AOP-400); and the Telecommunications Support and International Communications Division (AOP-600).

b. The AF IRM Division is responsible for the management of the Headquarters AF local-area network (LAN) and establishes requirements and procedures to enable the implementation of LANs and interfaces to Wide Area Network (WAN) in compliance with agency directives and guidelines.

c. Designated AF IRM Representatives are responsible for the design, implementation, maintenance and management of local and regional networks in coordination with local organizations.

2-10. DATA MANAGEMENT ROLES AND RESPONSIBILITIES.

a. The AF IRM Division is responsible for implementing an AF-wide Data Management Program that includes the establishment of data standards, the development and use of standard data dictionaries, the horizontal integration of corporate data assets, and the development of standard data access mechanisms and applications.

b. Designated AF IRM Representatives are responsible for the local implementation and management of the Data Management Program described above.

c. Program Managers for major systems are responsible for maintaining the integrity of data on their systems and for implementing required data management policies and procedures.

2-11. CONFIGURATION MANAGEMENT (CM) ROLES AND RESPONSIBILITIES.

a. The AF IRM Division is responsible for coordinating the establishment of functional configuration and configuration management standards and guidelines. Required CM procedures will be consistent with national requirements and standards.

b. Designated AF IRM Representatives are responsible for the implementation of the above standards. Specifically, they are responsible for managing network configurations, desktop configurations and any software configurations under their control. All of these configurations must meet established configuration management standards and security standards and must abide by all copyright laws. IRM Representatives are authorized to prohibit the use of hardware or software that does not fall within these guidelines and standards.

2-12. INFORMATION SYSTEMS DEVELOPMENT AND MAINTENANCE ROLES AND RESPONSIBILITIES.

a. The AF IRM Division is responsible for establishing Information Systems Development guidelines, requirements, and procedures.

b. The AF IRM Division is responsible for reviewing major Information Systems Development and Acquisition Plans, and monitoring development efforts for compliance to above standards.

c. The AF IRM Division is responsible for the development and maintenance of information systems needed to support corporate access requirements, e.g., Executive Information Systems.

CHAPTER 3. PLANNING AND BUDGETING

3-1. GENERAL.

IRM planning within AF encompasses all major activities covered by the Paperwork Reduction Act (PRA), all applicable FIRMR regulations, and all pertinent DOT and FAA orders. Since information resources play a major role in meeting AF and agency goals and mission objectives, they are an integral part of overall program, planning and management. To facilitate the integration of information resources with major AF program plans, AF addresses information and automation planning within several agency-wide planning processes. Collectively, these planning processes cover all major FAA strategic and tactical plans for information resources.

3-2. INFORMATION RESOURCES MANAGEMENT PLANNING DOCUMENTS.

IRM planning establishes AF IRM goals, objectives, strategies, implementation plans, and budgets for AF investments in information resources. This Order addresses requirements defined in the AF IRM Functional Plan.

a. Airway Facilities Information Resources Management Functional Plan. The AF IRM Functional Plan describes the AF IRM mission, mandates, vision, and strategies for the future. It is a long-term, strategic plan for AF IRM with a six-year time frame. It presents a set of action plans, both long term and tactical in nature, that drive the IRM program. The strategies and action plans will be updated every two years.

b. Airway Facilities IRM Five-Year Plan. The PRA and other federal directives require annual submission of five-year IRM plans describing anticipated information technology expenditures. This data is compiled by DOT to meet OMB A-11 reporting requirements. The AF IRM Division is responsible for compiling AF-wide 5-year plans for AIT based on submissions from regional offices, centers, and headquarters services.

c. Documented Plans that Impact AF IRM Planning. Other planning products that affect AF IRM planning processes include:

(1) Telecommunications Strategic Plan.

(2) The Airway Facilities Strategic Plan.

(3) Air Traffic System Capital Investment Plan (CIP) (Formerly titled National Airspace System Plan).

(4) Research Engineering and Development Plan (RE&D).

(5) FAA Corporate Information Technology Strategic Plan.

3-3. STRATEGIC PLANNING ENVIRONMENT.

Many offices and groups at headquarters, region, and sector levels will have input in the strategic planning process as pertains to IRM. These include:

a. The AF IRM Division. The AF IRM Division has overall responsibility to coordinate and integrate the efforts of the program organizations into a cohesive AF-wide IRM program.

b. Designated AF IRM Representatives. Regional, Center and Headquarters Directorate Information Resources Managers (IRMs) are responsible for coordination of all IRM-related activities within their program organization.

c. The FAA Office of Information Technology (AIT). AIT is responsible for coordinating FAA planning and implementation of IRM.

d. DOT Information Resources Management Office. The DOT office for IRM policy and oversight was established in DOT H 1350.2, The Departmental Information Resources Management Manual (DIRMM), as a central source for all DOT IRM policy.

e. Office of Management and Budget's Office of Information and Regulatory Affairs. This organization was created by the Paperwork Reduction Reauthorization Act of 1986 (P.L. 99-500). One of the express

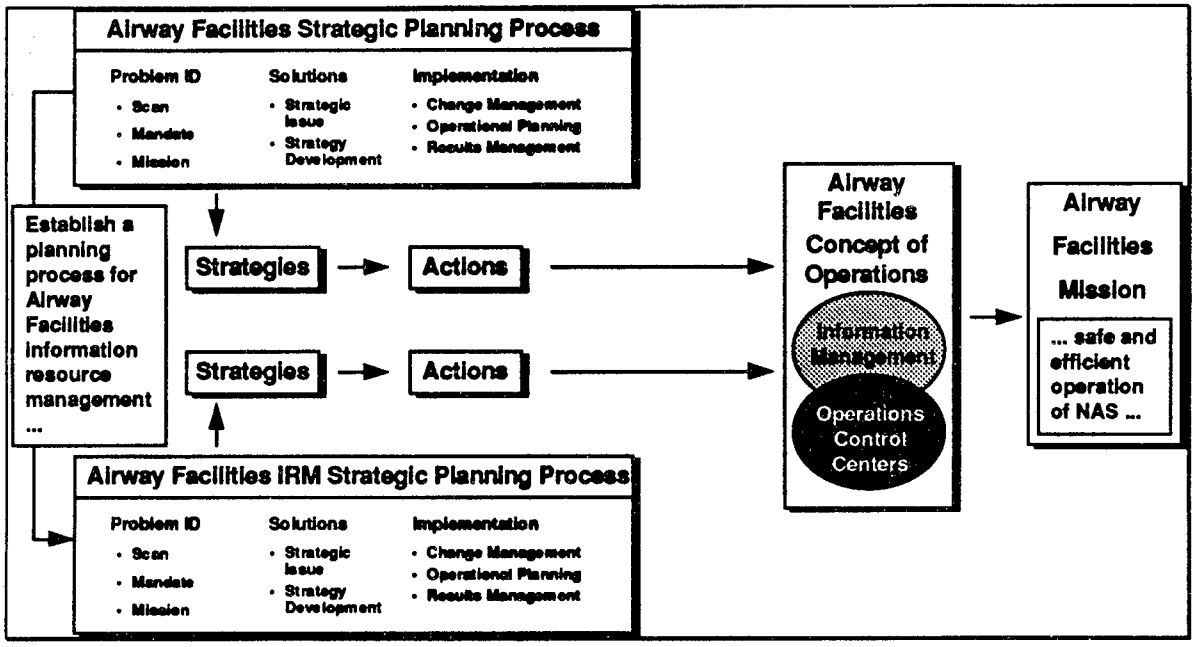
purposes of the law is to "improve Federal information policy making."

3-4. IRM STRATEGIC PLANNING – ROLES AND RESPONSIBILITIES.

a. General. IRM Planning within the FAA, and particularly within AF, has been established by a variety of orders, regulations and laws. With AF's decision to become an "operations-based" organization, the need for informed decisions and planning within the IRM realm has increased. In order to meet this need, IRM strategic planning processes must be understood and accepted by all of the parties involved.

c. Designated AF IRM Representatives. Designated AF IRM Representatives for the Regions, Centers, and Headquarters Directorate are responsible for implementation of AF strategies and action plans for IRM. Operational decisions for IRM shall be guided by existing IRM policies and procedures as well as strategies defined in the AF IRM Functional Plan. As stakeholders in the AF IRM Representatives, the AF Executive Resource Committee (ERC), and AIT in setting national IRM requirements and procedures, and in planning for future changes.

Figure 3-1. IRM and Airway Facilities Strategic Planning



b. AF IRM Division. The AF IRM Division, part of the Resources Management Directorate, oversees all planning functions for AF IRM. These functions include those assigned in FAA Order 1370.52C and FIRMR part 201-20, which prescribes policies and procedures regarding administrative programs for planning, organizing, and controlling resources for agency FIP requirements. The Division is also responsible for Headquarters Directorate IRM functions, including system architecture, automation, and acquisition. The Division shall coordinate with the designated strategic planning process, the designated AF IRM Representatives also contribute to the development of AF-wide strategies and implementation plans for AF IRM.

3-5. STRATEGIC PLANNING PROCESS.

Strategic planning for IRM has evolved from the planning process established3-ch for AF. As shown in Figure 1, the initiation of an AF IRM planning process was one of the actions mandated by the AF Strategic Plan.

a. Strategic Planning Methodology. The AF and AF IRM processes for strategic

planning follow the model selected and tailored to FAA requirements by the FAA Academy. The AF IRM Management Team is composed of representatives from the regions, centers, and headquarters. The Management Team carried out the initial strategic planning process that identified the initial set of strategies and actions required to address the mission requirements of AF. The process will be revisited on a biannual basis to update and revalidate IRM strategies and actions in light of the continually changing environment of AF IRM. The AF IRM strategic planning process is shown in Figure 2. It is based on the strategic planning model defined in John M. Bryson, *Strategic Planning for Public and Nonprofit Organizations,* (Jossey-Bass, San Francisco, 1988).

b. AF IRM Functional Plan. The major output of the strategic planning process is the AF IRM Functional Plan. The Functional Plan identifies strategies and associated actions that will guide IRM activities within AF. The strategies address IRM requirements for meeting AF program objectives. The actions and strategies define priorities for AF IRM investments.

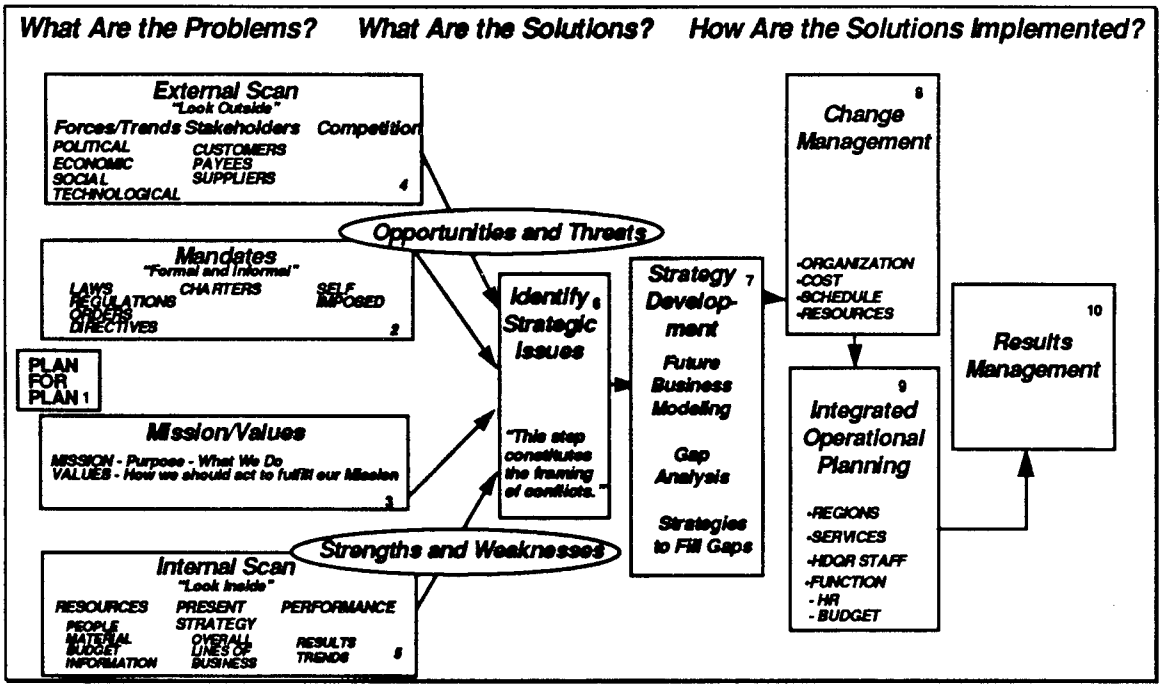
c. AF IRM Program Plan. The AF IRM Division shall develop an annual program plan to implement the strategies and actions defined in the AF IRM Functional Plan. The AF IRM Program Plan shall be consistent with timetables and other requirements in the Functional Plan.

d. Regional IRM Implementation Plan. Designated AF IRM Representatives shall develop implementation plans, consistent with requirements in the Program Plan, for their areas of responsibility.

3-6. BUDGET PLANNING.

a. Annual IRM Budgets. Annual IRM budgets reflecting anticipated headquarters and regional IRM requirements shall be prepared by designated AF IRM Representatives. Budgets shall identify and budget for all appropriate costs including training, maintenance, and other support requirements. The

Figure 3-2. Strategic Planning Process Model



AF IRM Division shall provide guidance as required for budget formulation.

b. All IRM related budget information shall be submitted to the appropriate organizations in a timely fashion to meet AF, FAA, DOT, OMB, and GSA reporting requirements.

c. AF IRM budgets for acquisition plans shall conform to requirements of FIRMR part 201-16, which requires agencies to prepare and submit annual agency-wide FIP plans to the OMB and GSA.

CHAPTER 4. ACQUISITION MANAGEMENT

SECTION 1. GENERAL REQUIREMENTS FOR ACQUISITION MANAGEMENT

4-1. GENERAL.

This section concerns Federal Information Resources Management Regulations (FIRMR) procedures and related FAA/DOT management approval requirements for acquiring *FIP resources* including hardware, software, services, and communications equipment and services. The Acquisition Requirements in this chapter supplement the provisions of Order DOT H.1350.2 and FAA Order 1370.52C, Information Resources Management—Policies and Procedures, and FAA Order 1810.1F, Acquisition Policy. Required information pertaining to delegation of procurement authority provisions are specified in FIRMR Part 201-39.

4-2. SCOPE.

This section applies to all AF programs within the scope of this Order, which have requirements and planned initiatives for procuring FIP resources, external or internal to the FAA. This section applies regardless of the method of acquiring the equipment, software, or services, including external procurements, integration of COTS software and in-house development. Specifically, it applies to AF procurements, procurements conducted via interagency agreement, project planning agreements (PPA), general working agreements (GWA), and contractor or other third party source agreements. The provisions of this chapter apply without regard to the manner and source of funding or organizational control over the procured services. Acquisitions are required to conform to requirements specified in all chapters of this Order, as well as related FAA and DOT orders.

4-3. EXTERNAL COMPLIANCE AND RELATED PUBLICATIONS.

a. The Federal Information Resources Management Regulation (FIRMR), issued by GSA, is the primary regulation governing the management, acquisition, and use of ADP and telecommunications resources by Federal agencies regardless of application. Acquisition provisions are specified in FIRMR Part 201-20. The regulation also covers Government-acquired ADP resources provided to contractors. The resources which are covered by FIRMR provisions include: FIP equipment, software, related supplies, maintenance services, FIP services, FIP support services, and telecommunications facilities and services. The FIRMR also includes direction of Government-wide FIP management information systems designed to satisfy management responsibilities with respect to effective and efficient acquisition, operation, and use of FIP equipment.

b. AF acquisition procedures shall conform to requirements described in the Federal Acquisition Regulation (48 CFR), Order DOT H.1350.2, FAA Order 1370.52C and FAA Order 1810.1F. For major acquisition programs expected to exceed $50 million, the acquisition must also meet requirements of the Key Decision Point (KDP) process specified in DOT's Major Acquisition Policies and Procedures (MAPP), Order DOT 4200.14C. In addition, the provisions of Transportation Acquisition Manual 1215.6, Source Selection, may apply if the acquisition is competitively negotiated.

4-4. OBJECTIVES.

a. The AF IRM Division aims to establish clear procedures and lines of authority within AF in order to manage the acquisition of Information Technology (IT) resources needed for meeting AF mission requirements. Because of the large expenditures involved in AF IT acquisition, improvement in the acquisition process offers substantial opportunities for cost savings as well as improved quality of the IT resources that serves AF mission requirements.

b. Acquisition policies and procedures are established to:

(1) Ensure that acquisitions support AF mission needs. .

(2) Reduce risk that acquisitions of AF information systems will fail to meet schedule and AF functional requirements.

(3) Ensure that consistent processes for review and execution will be applied to all AF acquisitions.

(4) Prioritize acquisitions and assist with AF planning.

(5) Monitor development and implementation of acquired technology and services.

4-5. GENERAL ACQUISITION REQUIREMENTS.

a. All acquisitions shall conform to requirements for Information Systems Development, Data Management, Configuration Management, Data Communications, Standards Implementation, Security, and other IRM requirements as specified in this order.

b. Acquisition plans for major systems shall be developed in response to AF mission requirements and as a result of analysis of requirements for business process improvement.

c. IT resources, including equipment, software, training, and contractor services, shall be acquired and used in the most efficient and effective manner consistent with the performance requirements of acquired information systems.

d. Requirements for major items of FIP equipment, software applications and services shall be anticipated well in advance of actual need and documented in long-range plans.

e. AF contractors shall not be allowed to acquire IT resources for the FAA that are not related to the performance of their contract. Use of contractor acquired equipment during and subsequent to contract fulfillment shall conform to requirements of the FAR (48 CFR) chapter 45, Government Property and applicable DOT and FAA policies .

f. IT resources shall be acquired by the method, conforming to appropriate procurement regulations, that offers the greatest advantage to the FAA.

g. IT resources shall be acquired competitively unless fully justified in accordance with applicable procedures.

h. Acquisition processes and management of contracts shall meet requirements for information system development and maintenance as described in Chapter 9 of this Order.

i. Acquisition plans shall document life cycle system requirements and costs, including needs to maintain and modify information system functionality, verify, and update data resources associated with or dependent on the acquired information system.

j. Users shall be actively involved in the development and evolution of operational requirements and in the planning and execution of Operational Testing and Evaluation (OT&E).

k. When warranted by program size, AF acquisition processes shall conform to requirements of the DOT Key Decision Point Process and related requirements described in FAA Order 1810.1F. These include:

(1) Regular revalidation of mission need, operational requirements, and program affordability at each key decision point.

(2) Consideration of all life-cycle costs in developing realistic cost estimates for programs.

(3) Program risk to be assessed explicitly at each key decision point prior to approval to proceed to the next acquisition phase.

(4) Realistic program schedules to ensure accurate projections of funding needs.

(5) Active tracking of contractor performance.

(6) A definition of requirements that begins with a well justified description of the operational deficiency.

(7) Maximum satisfaction of mission requirements through the use of non-developmental items (NDI) and COTS items when such products meet user and sponsor needs, including reliability and supportability.

In general, software products shall be acquired in the following order or priority:

(a) Government furnished software.

(b) Modification of existing government-owned software products.

(c) COTS.

(d) Integration of reusable software components and COTS products.

(e) New development.

(8) Developmental testing to verify attainment of technical performance requirements and operational testing to demonstrate operational effectiveness and suitability.

(9) Independent oversight of Operational Testing and Evaluation.

4-6. OVERVIEW OF FAA KEY DECISION POINT PROCESS.

a. The FAA acquisition process and procedures are described in detail in FAA Order 1810.1F. The process is defined in terms of familiar stages of phased development. For the largest acquisitions (Level I, IIIA, and IVA programs defined in 1810.1F) the phases consist of:

(1) Mission Need Determination.

(2) Concept Exploration.

(3) Demonstration and Validation.

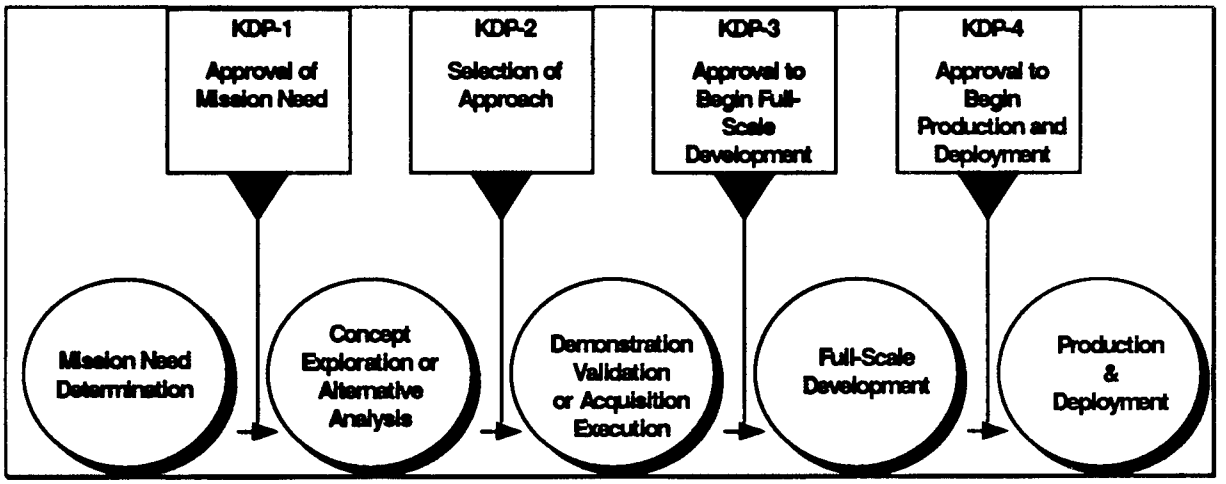
(4) Full-Scale Development.

(5) Production and Deployment.

b. For acquisitions involving technical and managerial support and for research programs (Level IVR acquisitions in FAA Order 1810.1F), a simpler process is employed.

c. The phased acquisition process is controlled by the Key Decision Point (KDP) Process (described in Order 1810.1F). Specific requirements for proceeding to successive phases are provided in the Order. The KDP Process is depicted in Figure 4-1. For each decision point, specific criteria for succeeding to a later stage in the process are provided. The process is designed to ensure that passing from one acquisition stage to another is justified by a continuing mission need and by meeting criteria that will enhance the likelihood of satisfying mission requirements and budgetary constraints.

Figure 4-1. Key Decision Point Process



4-7. PROJECT INITIATION.

A system development project can be initiated at any time. The Program Manager shall include major development projects in budgetary submissions. When the project is considered a major system or if the estimated life cycle cost is greater than the established AIT threshold for review of new systems, the Program Manager shall send the documented

request to the AF IRM Division for review of the project's conformance to IRM requirements. Other project requests are delegated to the designated IRM Representative for review.

4-8. DOCUMENTATION AND REVIEWS OF NEW INFORMATION SYSTEMS ACQUISITIONS.

The acceptance of the project request constitutes approval to proceed with the required Requirements Analysis and Analysis of Alternatives. The Program Manager initiates these studies and prepares the associated documentation to support project initiation, described below and in Chapter 9 of this order.

a. Acquisition Documentation. AF program offices shall submit relevant acquisition documents to the AF IRM Division in the course of delivering required documentation to other review organizations. Such documentation shall be accompanied by a statement identifying specifics that may be required in the case that an acquisition does not conform to DOT, FAA, AIT or AF IRM requirements. Program Managers for major systems are responsible for submitting all acquisition documents that may impact AF IRM plans or operations. Such documents include:

(1) Mission Need Statement.

(2) Information submitted to AIT for inclusion in the Information Resources Management Plan.

(3) Operational Requirements Document.

(4) Acquisition Plan.

(5) Program Implementation Plan.

(6) Integrated Logistics Support Plan.

(7) Risk Management Plan.

b. IRM Review. The AF IRM Division shall review AF acquisition plans for new automated information systems and major modifications of existing systems. The review shall ensure that acquisition plans do not duplicate existing information system functionality and that the plans are consistent with AF IRM requirements. Other review bodies shall evaluate non-IRM acquisition requirements, such as satisfaction of mission need and life-cycle cost estimates.

c. Small System Acquisitions. Requests for development efforts and acquisitions, under the established threshold for AFZ-500 and higher level approval, shall be reviewed and approved by the designated AF IRM Representative and other appropriate approving authorities. These acquisitions shall also meet standards, regulations, and other AF IRM requirements and demonstrate that the proposed expenditure does not duplicate an existing information system.

4-9. ACQUISITION REQUIREMENTS SUMMARY.

a. Specific guidance for acquisitions procedures are provided in FAA Order 1370.71A, Federal Aviation Acquisition Manual Bulletins FB 93-09 and FB 93-04 in addition to requirements specified in FAA Order 1810.1F.

b. All acquisitions shall conform to relevant requirements in this order. Specific approval authorities shall conform to GSA, DOT, and FAA requirements. Guidelines for approval requirements and authority shall be provided in acquisitions guidelines from the AF IRM Division.

SECTION 2. ACQUISITION ROLES AND RESPONSIBILITIES

4-10. AF IRM DIVISION.

a. The AF IRM Division is responsible for the establishment and oversight of IT acquisition guidelines and procedures for AF. The primary focus of the oversight for acquisition is to ensure that all AF IT acquisitions meet both functional performance requirements and also requirements specified in the AF IRM Strategic Plan and in the AF

Strategic Plan. The AF IRM Division shall be responsible for defining standards for AF acquisition, monitoring acquisition processes, and facilitating improvement in those processes.

b. The AF IRM Division is responsible for monitoring and coordinating acquisition functions that are carried out within the regions and centers. Key areas of AF IRM Division responsibility include the following:

(1) Monitoring conformance of AF acquisition processes and documentation to FAA and DOT regulations and requirements.

(2) Evaluating requests for resources within AF. Various other AF authorities are involved in evaluating and approving requests for IRM expenditures. They include: AAF-1, the Executive Board, designated AF IRM Representatives, Program Managers for major systems, as well as higher-level decision making bodies within the FAA and DOT.

(3) Criteria that apply to evaluating acquisitions include:

(a) Impact on AF core business processes--short-term benefits and strategic impact.

(b) Risks related to business impact (benefit risk).

(c) Risks related to application development.

(d) Timeframe for benefit (priority on short-term impact).

(e) Timeframe for development.

(f) Longevity of acquired technology.

(g) Resource requirements (priority on small-scale investments).

c. Establishing requirements for acquisitions in relation to long-range AF and FAA objectives for IRM. Such requirements include:

(1) Conformance of acquisitions to requirements for FAA Open Systems Environment (OSE).

(2) Implementation of training programs.

(3) Planning for changes in business processes needed to take advantage of new technical capabilities.

(4) Meeting AF and FAA standards and procedures for Data Management.

(5) Meeting FAA and AF requirements for reusability of newly acquired software.

(6) Delivery of documentation and other acquired products in standard appropriate electronic format.

d. Monitoring conformance of AF acquisitions to AF requirements and evaluating requests for waivers.

e. Applying metrics for acquisition processes in order to evaluate effectiveness of acquisition policies and procedures.

4-11. AF REGIONAL ACQUISITION ADMINISTRATION.

The AF IRM Representatives for the regions, centers and Headquarters Directorates shall be responsible for the implementation of acquisition policies and procedures within their organizations. In addition to the shared responsibilities described above, regional responsibilities include:

a. Coordination of acquisition planning for regions, centers and Headquarters.

b. Evaluation and prioritization of proposed acquisitions in relation to federal acquisition policies and AF requirements.

c. Monitoring acquisition processes.

4-12. AF PROGRAM MANAGERS FOR MAJOR SYSTEMS.

The Program Managers for major systems exercise the major responsibility for identifying requirements for AF acquisitions and for ensuring that acquisitions meet AF functional requirements. Special areas of responsibility for Program Managers include:

a. Development of acquisition proposals and related documents.

b. Monitoring contractor schedules and performance.

c. Overseeing OT&E for acquired IT resources.

d. Development of implementation plans for acquired IT resources, including training and support.

CHAPTER 5. DATA MANAGEMENT

SECTION 1. GENERAL REQUIREMENTS FOR DATA MANAGEMENT

5-1. GENERAL.

a. High quality information delivered when and where required is essential for AF to fulfill its business mission. Data management is the discipline that enables an organization to use information systems to acquire, manipulate, analyze, store, retrieve, and distribute information required to meet the organization's mission. Data management consists of two principal organizational functions, data administration and database administration. Data administration encompasses defining, organizing, managing, controlling and protecting data, but does not include processing of data. Database administration encompasses defining, organizing, managing, controlling, and protecting databases.

b. This chapter primarily addresses requirements for data administration. Carrying out appropriate data administration policies and procedures shall implement practices for database management, which are consistent with the broader data management requirements of AF.

c. Policies and procedures for data management have a wide impact on the entire life cycle of information systems development (ISD). While the requirements for ISD are described in Chapter 9, the requirements for data management apply to all automated systems which generate or change data that resides in AF databases within the scope of this order.

5-2. RELATED PUBLICATIONS.

Other sources that provide more detailed descriptions of data management procedures include:

a. National Institute of Standards and Technology (NIST), Manual for Data Administration, Special Publication 500-208, March 1993.

b. NBS Special Publication 500-149, Guide on Data Entity Naming Conventions.

c. DoD, Data Administration Procedures, DoD 8320.1-M December 1992.

d. Data Standards, Order 1375.1B.

e. Standard Data Elements and Codes, General Standards, 1375.2A; Change Notice 1.

f. Standard Data Elements and Codes, Airport Standards, 1375.3B; Change Notice 1.

g. Standard Data Elements and Codes Facility Identification and Supplemental Standards, Order 1375.4A; Change Notices 1-4.

h. Standard Data Elements and Codes, Accounting, Order 1375.6A.

i. Organization/Cost Center Codes Standard Data Elements, Order 1375.7A.

j. NBS Special Publication 500-149, Guide on Data Entity Naming Conventions.

k. Information Resource Dictionary System (IRDS) Supplement to ANSI X3.138A-1991. FIPS/ANSI; April 5, 1989, ANSI X3.138-1988, FIPS PUB 156.

l. Data Standards and Guidelines/Representations and Code Set, FIPS PUB 19-2.

5-3. SCOPE.

As identified in Chapter 1, this order addresses requirements for all AF information systems except those directly concerned with real-time Air Traffic operations. The data management requirements pertain to all data under the control of AF that contribute to AF operations and decision-making processes. It should be noted that national information systems under AF program management are subject to national program requirements and standards as well as AF IRM requirements.

5-4. FUNDAMENTAL ASSUMPTIONS OF DATA MANAGEMENT.

The policies, guidelines, and procedures outlined below follow from certain basic assumptions on the management of AF information.

a. **Timely, accurate, secure data is a basic asset of AF** that must be managed to serve AF mission objectives.

b. **Data is a resource that is shared** among organizations (e.g., AF regions), functions, personnel, and information systems.

c. **Information should be collected and managed by those closest to the source of the data.** Data is collected at the source only once and is validated for correctness and conformance to requirements and standards at the source.

5-5. DATA MANAGEMENT OBJECTIVES.

AF IRM procedures and practices shall meet the following objectives in support of the FAA Corporate Data Management Program:

a. To maintain data standards and systems capabilities that permit transparent access to data by all authorized users.

b. To provide for accuracy, currency, quality, consistency, and security of data required for AF business processes.

c. To store data in authoritative, shared, and non-redundant databases.

d. To facilitate sharing and accurate interchange of data within the FAA, and between FAA organizations and external organizations and systems.

e. To minimize cost of acquiring and maintaining data.

f. To promote rapid development and modification of Information Systems (IS) applications that support AF business requirements by means of data standardization and standard methods for data access.

g. To provide services in support of these objectives in a cost-effective and reliable manner.

5-6. GUIDELINES FOR DATA MANAGEMENT.

a. **Strategic focus of AF Data Management.** AF guidelines and procedures for data management shall be consistent with requirements of the AF business mission and with FAA, DOT, and other federal policies for data management, including the FAA Corporate Data Management Program, Corporate IT Strategic Plan, and the FAA Strategic Plan.

b. **AF Data Architecture.**

(1) The AF data architecture specifies how information shall be managed, organized, and defined. The architecture also specifies how automated systems shall be used to support the acquisition, management and delivery of information to users in support of the mission, goals, objectives, functions, and decision-making processes of the organization. The data architecture shall include specifications for: data elements, databases, an information repository, and electronic data interchange.

(2) The architecture provides for a common set of information concepts for integrating data definitions across organizations, locations, functions, and information systems. It provides a description of entities, attributes, and relationships among entities and corresponding databases.

(3) The architecture provides a foundation for incremental, verifiable processes for development of systems of mutually consistent subject databases based on successively more detailed levels of data modeling.

(4) AF guidelines and procedures for data management shall support implementation of corporate systems architecture requirements as defined by AIT and the AF IRM Division.

c. **Data Standards.** Data standards and the policies and procedures that support them are an important part of the requirements for interoperability. Data standards complement data communications standards, such as Government Open Systems Interconnection Profile (GOSIP), which are designed to implement an FAA OSE within all

federal agencies. AF shall follow standards established by NIST and other Federal, DOT, and FAA standards. Data standards shall apply to:

(1) Data element standards, including data naming conventions and other meta-data requirements. ("Meta-data" refers to information about the data stored in information systems.)

(2) Data management terminology and definitions.

(3) Data modeling and architecture conventions.

(4) Data management standards for system development and life cycle maintenance.

(5) Data documentation for meta-data and data inventories.

(6) Standards for data content such as documentation, graphics, and specifications in support of Electronic Data Interchange (EDI).

d. Data Management Responsibilities. Data management must be based on clearly defined responsibilities and accountabilities. Data management and quality control should be the responsibility of those most knowledgeable about the substance of the information; i.e. the generating source. Managers at all levels of AF are responsible for ensuring that AF data management guidelines and procedures are carried out in support of AF missions.

e. Data Life Cycle. Standard procedures shall be followed for the entire "data life cycle" including generation and acquisition of data, maintenance of data, and retirement of data.

f. System Development and Data Models. Data management principles and procedures shall be applied in the course of systems development. Applications shall be based on the use of approved data models for database design and implementation.

g. Configuration Management of AF Data. Processes that authorize and monitor changes to AF corporate data shall follow accepted policies and procedures for configuration management.

h. Electronic Records Management. Records management is the corporate foundation for the management of information and must be incorporated into all levels of IRM planning and development. Storage, maintenance and disposal of electronic corporate data shall follow appropriate FAA and DOT policies and procedures for management of records stored on FIP equipment and associated media.

i. Management of Shared Data . The management of data as a shared FAA resource requires a major "cultural" change in the way in which information is generated and maintained. AF information systems strategies shall meet the following objectives:

(1) Data should be collected, entered, and validated only once, as near as possible to its source.

(2) Data should be stored in shared, non-redundant databases.

(3) Maintenance procedures and information system designs should ensure that changes to data in one information system database results in accurate and timely changes to dependent information in all FAA databases.

j. Maintenance of the AF Information Repository. The AF Information Repository, which tracks and maintains rules for data content, is a key tool for enhancing the ability to share data and maintain data integrity. Program Managers for major systems are responsible for creation, validation, and maintenance of data contained in automated information systems under their control. AF databases and information systems will be designed and maintained to conform with FAA and AF information repository requirements.

k. Data and Total Quality Management (TQM). AF shall maintain standards and processes for data quality and ensure that such processes are integrated with related TQM efforts. Measures of data quality include timeliness, accuracy, ease of access and use, and conformance to data rules.

SECTION 2. DATA MANAGEMENT ROLES AND RESPONSIBILITIES

5-7. GENERAL.

AF Data Management guidelines and procedures are designed to ensure that functional data serves AF mission objectives. Anyone authorized to acquire or change AF corporate data has a responsibility to maintain the integrity of that data. Specific individuals include the AF Data Management Program Officer, the designated IRM Representatives and Program Managers for major systems. AF managers have responsibility to ensure that AF personnel are properly trained and supervised in prescribed data management procedures.

5-8. AF IRM DIVISION RESPONSIBILITIES FOR DATA ADMINISTRATION.

The AF IRM Division, and the Division's designated Data Management Program Officer, are responsible for overall coordination of IRM requirements and procedures within AF, including planning the Data Management strategy for AF and ensuring that resources are budgeted and applied to carrying out the strategy. The AF IRM Division also monitors implementation of federal data management policies and specific AF requirements, and modifies strategies and implementation plans as warranted to meet AF data management and other IRM objectives.

a. Data Management Planning. As part of its AF IRM planning function, the AF IRM Division shall coordinate AF Data Management planning and develop appropriate data management procedures to meet AF mission objectives. The AF IRM Division is responsible for the production, modification, and configuration management of products related to IRM planning and supervision. Areas of responsibility and products of the planning process include:

(1) Annual Strategic Plan and Guidance for AF Data Administration.

(2) Orders that prescribe procedures, standards and other requirements for Data Management.

(3) Periodic program assessments.

(4) Migration plans for existing (legacy) data where such data does not conform to AF data standards.

(5) Strategies and plans for Data Management process improvement.

(6) Business cases for Data Management strategies and programs.

(7) Implementation plans for Data Management processes.

(8) Plans and budgets for procuring required Data Management program resources.

b. Maintenance of the AF Information Repository. In order to maintain consistency and accessibility among AF data sources, AF shall implement and maintain a facility for tracking information on the data residing in AF databases. The AF repository shall build upon corresponding AIT efforts in corporate data management. Specific responsibilities include:

(1) Development of a complete inventory of uniquely identified and accurately defined information resource entities and attributes. AF shall follow a standard process for identifying and defining information resource entities, the basic units of information that are stored and managed in formal database systems. An established standard process shall also be used to maintain the resulting information resource entity meta-data (data that identifies and describes the content of data elements).

(2) Implementation and maintenance of an AF Information Repository. The repository tracks where the entities are used, the frequency of use, and the rules that constrain their use during all phases of the life cycle. The AF Information Repository shall be consistent with FAA Information Repository requirements.

(3) Management of the interface to the FAA Information Repository.

(4) Providing assistance to designated IRM Representatives and Program Managers for major systems with data naming and standardization.

(5) Providing services and procedures that facilitate access to repository data.

c. Establishment of standard practices to model AF data requirements. Effective Data Management depends on identifying the data required to perform business processes. While the definition of those processes is the responsibility of the program managers, the AF IRM Division shall establish an approach, consistent with FAA standards, for modeling the processes and related data. The models support efforts to share information among AF functions. Process and data models for AF functions contribute to the development of AF and FAA composite models required for development of the AF Information Repository (for AF meta-data). The composite models shall be used to define naming conventions for data, required for AF-wide data access. The models shall be consistent with FAA standards.

d. Establishment and monitoring of policies and procedures for data security. In compliance with FAA policy, AF practices for data security shall:

(1) Limit access to qualified users.

(2) Provide physical and administrative protection against fraud, disclosure, sabotage, and destruction of data.

(3) Establish and monitor procedures to backup and archive data in accordance with records management policies.

Detailed requirements for information security are given in FAA Order 1600.54B and in Chapter 8 of this order.

e. Establishment of specific procedures and standards to promote data sharing and interoperability among AF systems. To achieve these objectives AF shall:

(1) Build upon the OSE to provide for a common means for data access among AF and FAA information systems.

(2) Define and monitor the implementation of data standards and other requirements for interchange among standard systems without loss of content or meaning of data.

(3) Integrate AF procedures and standards with higher-level FAA, DOT, and NIST standards.

(4) Support functional managers in efforts to identify and locate data across AF systems.

(5) Establish and monitor quality metrics for Data Management.

(6) Initiate and monitor training in Data Management at all AF levels.

(7) Maintain information on data handling facilities and costs associated with data.

(8) Establish procedures to implement configuration management requirements for AF data.

(9) Encourage the acquisition and use of standard tools for modeling business processes and data. Such tools should produce meta-data consistent with information repository requirements. Guidelines for tool selection are provided in the NIST, Manual for Data Administration, Special Publication 500-208, Section 8.

f. Serving as a liaison to AIT. The AF IRM Division is responsible for maintaining relationships with AIT as required to maintain currency with relevant data management policies and standards.

5-9. AF REGIONAL DATA ADMINISTRATION.

The IRM Representatives for the regions, centers and Headquarters Directorates shall be responsible for the implementation of AF Data Management procedures and standards within their organizations. Specific Data Management responsibilities of the designated IRM Representative include:

a. Developing Data Management plans for implementing AF Data Management strategies and requirements.

b. Planning, programming, and budgeting for their organizations.

c. Serving as liaison to the AF IRM Division.

d. Implementing information repository systems and services including management and control of meta-data required to populate AF Information Repository.

e. Acquiring technology and automated tools to implement AF data standards and ensuring that the tools conform to AF requirements.

f. Reviewing and maintaining functional data models and standard data element names and descriptions.

g. Evaluating functional data proposed for adoption as standard AF and FAA data.

h. Supporting data sharing by identifying and maintaining data consistent with the requirements of the AF and FAA information repositories. The AF information repository will facilitate access to data by maintaining global directories and information on data definitions, locations, and relationships.

5-10. AF DATA ADMINISTRATION FOR MAJOR SYSTEMS AND PROGRAMS.

The Program Managers for major systems exercise the major responsibility for implementing AF Data Management procedures and standards and for maintaining data integrity for AF. The Program Managers for major systems are responsible for the processes that generate and maintain data in their specific domains. Data must be maintained in such a way that it remains a reliable AF and FAA asset for use by all authorized organizations and individuals who require access to the data. Specific areas of responsibility include:

a. Producing procedures to implement Data Management for specific AF functions.

b. Adapting standard data development processes for relevant functional areas .

c. Specifying procedures and standards to implement data quality processes for functional areas.

d. Conducting quality tests and evaluating test results.

e. Performing business process improvement analysis.

f. Developing process and data models.

g. Recommending process modifications to improve data quality and conformance to data standards and rules.

h. Supplying data to the AF Information Repository and recommending changes where required. Program managers shall make use of FAA and AF information repositories and shall ensure that data maintenance procedures conform to AF repository requirements. Information systems development programs shall establish an Interface Control Working Group (ICWG) within the development group to address the sharing of corporate data with other AF systems and customers.

i. Controlling changes to data including establishing configuration baselines and determining effects of change requests on data content and data models.

CHAPTER 6. CONFIGURATION MANAGEMENT

SECTION 1. CONFIGURATION MANAGEMENT FOR NETWORKS AND USER RESOURCES

6-1. GENERAL.

The term Configuration Management (CM) is used in two different contexts in this chapter. This section addresses the AF IRM Division's requirements for maintaining inventories and for tracking changes to hardware and software components, or configuration items, that are part of Local Area Networks (LANs) and associated user resources. The objective is to track and maintain the operational state of the AF LANs, and associated services and resources. Section 2 examines CM requirements for information systems development.

6-2. SCOPE.

Guidelines and procedures in this section apply to AF systems and networks not specifically covered by FAA Order 1800.8F, National Airspace System Configuration Management. The CM guidelines in this chapter supplement the national requirements for CM, including directives and guidance within FAA Order 1800.8F. CM applies specifically to:

a. Desktop and Other Information System Resources. A hardware or software item that either contains AF corporate data or affects network operations shall be subject to configuration control.

b. Network Resources. All AF servers and related hardware and software resources shall be subject to configuration control.

c. Software Development Resources. All systems under development, within the scope of this order, shall be subject to CM requirements as defined in this and other FAA orders.

6-3. RELATED PUBLICATIONS.

a. FAA Order 1800.8F, National Airspace System Configuration Management.

b. FAA Order 1800.63A, National Airspace System (NAS) Deployment Readiness Review (DRR) Program.

c. FAA Order 1600.54B, FAA Automated Information Systems Security Handbook.

d. FAA-Standard-021a, Configuration Management (Contractor Requirements).

6-4. CM OBJECTIVES AND BENEFITS

CM identifies systems components and aggregations, controls changes, and reports on the state of hardware and software systems at all stages of development, production, and operation. Properly executed CM shall:

a. Facilitate implementation of standards by controlling changes to hardware and software IT resources.

b. Maintain accurate information on IT resources in development and in operation.

c. Improve reliability by controlling changes in system configuration that may affect system and network operations.

d. Ensure conformance of implemented systems to specifications.

e. Reduce cost and time required for systems development by tracking and controlling changes in system components.

6-5. CM ROLES AND RESPONSIBILITIES.

a. The AF IRM Division participates in establishing CM procedures, providing oversight of CM practices, and ensuring that

appropriate levels of monitoring and auditing are performed at all levels throughout AF.

b. Program Managers for major systems shall ensure that established CM procedures are followed and that CM practices are instituted at the appropriate levels in their respective programs. The Program Manager shall ensure there is CM staff to perform CM activities.

c. Regional Managers shall ensure that established CM procedures are followed and that CM practices are instituted at the appropriate levels with regional consistency in their respective regions. Regional managers or Program Managers for major systems shall designate a CM representative to manage network and system configuration.

d. Designated IRM Representatives shall support CM procedures by reviewing, monitoring, and auditing established CM practices on a regular basis in their respective areas of responsibility.

(1) LAN Administration. When the LAN Administrator and the designated IRM Representative positions are held by the same person, that person shall authorize all changes to the LAN. When the positions are held by different people, the designated IRM Representative, in conjunction with the LAN Administrator, shall authorize changes to the LANs unless the change is ruled as major by the LAN Administrator.

(2) Desktop and Other Information Systems. The designated AF IRM Representative shall ensure that procedures are in place to manage and support changes to desktop and other information systems.

e. LAN Administrators shall review all changes to the LANs. Major changes, e.g., concerning the LAN structure or protocol, etc., shall be submitted to the designated IRM Representative or other appropriate Configuration Control Authority for review.

f. Developers of Information Systems and Other AF Employees shall adhere to established CM practices at their respective locations.

6-6. CONFIGURATION CONTROL AUTHORITIES.

These officials establish system and network baselines, approve or disapprove subsequent changes to those baselines, and track the status of change implementation. The AF Configuration Control Authority levels are:

a. AF IRM Division Configuration Control Authority. This official shall review and decide upon requested changes to the system and network configuration baselines that are AF-wide.

b. Program Manager Configuration Control Authority. This official shall review and decide upon requested changes to the system and network configuration baselines that are program-wide.

c. Regional Configuration Control Authority. This official shall be responsible for deciding which items are to be placed under configuration control, reviewing change requests, and authorizing implementation of approved changes.

6-7. CONFIGURATION STANDARDS FOR INFORMATION RESOURCES.

Each Configuration Control Authority shall define standards of hardware and software configuration items for both systems and networks. The core standards for desktop systems and LANs shall be the standard configurations established for NASMAP. All deviations from the standards shall be recorded and authorized by the appropriate configuration control authority. Several standard configurations may be defined to accommodate varying user requirements.

6-8. CM ACTIVITIES.

The following standard CM activities shall take place within every program and region for all new and existing systems and networks. The procedures in FAA Order 1800.8F for NAS CM should be tailored to the size and scope of the system or network.

a. Identification.

(1) Identification includes the names and serial numbers of all hardware and software (manuals and disks including those for COTS software) of each workstation and

location; identification of workstations attached to the network; and identification of the hardware and software components of each network. Definition of what component (hardware, software, data) constitutes a configuration item is determined by the Program Manager, subject to existing orders and policies, such as the NAS configuration hierarchy, and constraints imposed by related systems.

(2) Portable computers and resident software are included as configuration items. A system (manual or automated) shall be instituted that identifies the borrower/user of each portable computer to ensure that the location of the computer is known at all times.

(3) Each software package shall be identified as a unique configuration item. It is recommended that any changes made to commercial software by AF be identified and controlled in accordance with FAA-STD-021a, Configuration Management (Contractor Requirements). Changes to commercial software and associated documentation shall be proposed to the appropriate Configuration Control Authority and approved prior to implementation.

(4) Automated CM tools and network managers that poll attached workstations are recommended for use whenever possible.

b. Change control.

(1) All changes in hardware and software configurations of systems and networks shall be controlled by a unique number. Information collected shall consist of the date of request, date needed, date completed, description, and estimates of the time and dollar resources required to carry out the change.

(2) Equipment under configuration control should not be moved without prior authorization and all changes in location should be recorded in a timely manner. Authorization may be obtained from the designated CM representative following documentation of changes.

c. Status accounting. This process tracks and reports the progress of changes to a configuration item (proposed, approved, canceled, or implemented). Status accounting shall also generate various reports providing information on change proposals in the review process, approved changes that are in progress, and the current configurations of systems and networks.

d. Auditing. The configuration items of systems and networks shall be audited periodically to ensure that the actual configuration conforms to what is recorded.

e. Reporting. System changes shall be documented and reported to appropriate organizations and electronic systems. CM reports shall include:

(1) System and network configurations.

(2) Status of changes to the configurations.

6-9. DEPLOYMENT READINESS REVIEW GUIDELINES.

Prior to deployment of NAS systems and major corporate information systems, a Deployment Readiness Review (DRR) will be conducted to assess whether the system or subsystem is ready for deployment. The review will also assess training and other requirements for field implementation. All modifications to systems or documentation that have been specified or completed shall be controlled by CM procedures. The CM organization shall provide input to the DRR assessment plan. Refer to FAA Order 1800.63A for more information regarding the DRR process.

6-10. SOFTWARE LICENSING AND METERING.

In addition to the software licensing policy stated in FAA Order 1600.54B, paragraph 908, the following applies to AF systems and networks.

a. Software licensed for multiple users shall be metered. Each copy shall be assigned a unique number. Information recorded shall consist of the software name, the identification and copy numbers, and the workstation where it is installed. Metering of site licenses shall be carried out in accordance with licensing agreements by the relevant Configuration Control Authority.

b. Each user shall have a license agreement for all software applications installed including one for the operating system. When software is metered, each user shall have a copy of the license agreement with the copy's unique number noted.

c. When software is transferred from one system or network to another, the license, manuals, and disks shall accompany the transfer, and changes shall be recorded.

d. The multi-user license for application software on a LAN shall also be metered. At no point in time shall the number of users exceed the number of users licensed.

SECTION 2. SOFTWARE CONFIGURATION MANAGEMENT FOR IN-HOUSE SYSTEM DEVELOPMENT

6-11. GENERAL.

a. The requirements for CM for development, installation, and maintenance of NAS systems and subsystems are described in FAA Order 1800.8F, National Airspace System Configuration Management and FAA-Standard-021a Configuration Management (Contractor Requirements). This is the highest level CM policy for the FAA.

b. Non-NAS systems, whether developed in-house or developed under contract, must also follow appropriate CM practices This section describes the general CM process for information systems development and maintenance. The application of the process should be tailored to the size, complexity, risk, and mission criticality of the system placed under configuration control.

c. Software CM establishes and maintains the integrity of the software products of an AF corporate software development project throughout the project's life cycle. Directives and guidelines within this chapter are based on the key software CM practices adapted from the Software Engineering Institute's Capability Maturity Model for Software and FAA Order 1800.8F.

6-12. CATEGORIES OF SYSTEMS SUBJECT TO CM.

CM practices should be applied to meet the requirements of the following categories of systems:

a. **NAS Systems.** NAS systems are subject to the full set of requirements contained in FAA Order 1800.8F.

b. **Non-NAS Major AF Corporate Systems.** Non-NAS information systems developed by AF, which are major repositories of corporate information, are subject to configuration control as outlined in this section.

c. **Local Systems.** Small-scale systems developed on a local or regional basis are subject to configuration controls appropriate to the size and complexity of the system. In general, formal baselining will only apply to major corporate systems.

6-13. CM RESPONSIBILITIES.

The Program Managers for major systems shall implement required software CM practices on each software development project. CM procedures shall:

a. **Identify the software configuration items** of the software at given points in time. Configuration items include software products developed and those acquired to develop or run the product.

b. **Establish a software baseline library** that contains the baselines as they are developed or added.

c. **Control changes to the configuration baseline** via well-defined change control procedures and configuration auditing. This will thereby maintain the integrity and traceability of the configuration throughout the software life cycle.

6-14. CM OBJECTIVES.

The Program Managers shall support the following AF CM objectives:

a. To plan all software CM activities in compliance with AIT, FIP, and Open Systems Interconnection (OSI) standards.

b. To identify all software configuration items that require control and make them available to the affected people and groups.

c. To control all changes to software configuration used in system builds and operational systems.

d. To inform all interested parties of the status and content of system baselines.

6-15. KEY COMMITMENTS.

The Program Managers shall ensure for each software development project that there is:

a. Explicit assignment for the responsibility of software CM.

b. Software CM in existence throughout the system's life cycle.

c. Software CM of all reasonable items within the software configuration, i.e., products, tools, equipment.

d. Establishment and access to a repository for storing software configuration items and associated software CM records. Configuration items are decomposed into configuration components, then configuration units. An entire system may be considered to be a single one configuration item, which is then further decomposed into components and subcomponents. A system may also be viewed in terms of multiple configuration items. Definition of what constitutes a configuration item is determined by the Program Manager, consistent with other FAA requirements such as the NAS MD-001 configuration hierarchy.

e. Periodic auditing of baselines and CM activities.

6-16. SOFTWARE CONFIGURATION CONTROL AUTHORITY.

The Program Manager shall establish a software configuration board (for major systems) or configuration control authority for each software development project. Configuration control boards shall carry out responsibilities as outlined in FAA Order 1800.8F. The configuration control authority shall:

a. Authorize the establishment of baselines.

b. Identify configuration items, components, and units.

c. Represent the interests of the Program Manager and all system or software development groups who may be affected by changes to the baselines.

d. Review and authorize changes to baselines.

e. Authorize the creation of products from the baseline library.

6-17. SOFTWARE CM RESPONSIBILITIES.

The Program Manager shall designate an individual or establish a group responsible for coordination and implementation of software CM for each software development project. Such groups are composed of managers and individuals within the concerned organizations who have responsibility for a set of tasks or activities. The CM Manager or group shall:

a. Create and manage the software baseline library.

b. Develop, maintain, and distribute software CM plans, standards, and procedures.

c. Identify the work products to place under software CM. Work products result from defining, maintaining, or using a software process.

d. Manage access to the software baseline library.

e. Update baselines.

f. Generate products from the baseline library.

g. Record software CM actions.

h. Produce and distribute software CM reports.

6-18. RESOURCES AND FUNDING.

The Program Manager shall ensure that there are adequate software CM resources and that funding is planned and available for each software development project, specifically that:

a. A manager is assigned specific software CM responsibilities.

b. Automated tools shall be employed to support software CM.

6-19. SOFTWARE CM GROUP TRAINING.

The Program Manager shall ensure that members of the software CM group are trained in the objectives, procedures, and methods for performing software CM activities. Subject areas for training shall include software CM standards, procedures, methods, and tools.

6-20. OTHER SOFTWARE-RELATED GROUPS TRAINING.

The Program Manager shall ensure that members of the engineering, quality assurance, and documentation support groups are properly trained in CM processes. Training shall include:

a. Software CM standards, procedures, and methods to follow for CM activities inside these groups.

b. Software CM roles, responsibilities, and authorities for the software CM group.

6-21. ACTIVITIES.

For major development efforts the Program Manager shall oversee the following CM activities:

a. **Prepare a software CM plan.** The plan shall be:

(1) Developed in the early stages of the overall project planning.

(2) Reviewed by affected groups.

(3) Modified in accordance with accepted change control procedures.

b. **Use a documented and approved software configuration plan** as the basis for performing software CM activities. The plan covers:

(1) Software CM activities to perform, the schedule of activities, the assigned responsibilities, and the resources required (personnel, equipment, tools, space).

(2) Software CM requirements of performance by the software engineering group and other development-related groups.

c. **Use an established software CM library system as a repository for the baselines.** Several projects may use one library system as long as multiple projects can be supported. This library system:

(1) Supports multiple control levels of software CM. Examples of multiple-level-control situations are:

(a) Different times in the life cycle may require different levels of control, e.g., tighter control as the product matures.

(b) Software-only systems require less control then systems with both hardware and software.

(2) Provides for storage and retrieval of configuration items, components, and units.

(3) Provides for sharing and transfer of configuration items, components, and units between the affected groups and between control levels within the library.

(4) Helps in the use of product standards for configuration items, components, and units.

(5) Provides for storage and recovery of archived versions of configuration items, components, and units.

(6) Helps to ensure correct generation of products from the baseline library.

(7) Provides for storage, update, and retrieval of software CM records.

(8) Supports production of software CM reports.

(9) Provides for maintenance of the library structure and contents. Examples of maintenance functions include backup and restoring of library files and recovery from library errors.

d. Identify the products to be placed under software CM. The configuration items, components, and units are:

(1) Selected based on documented criteria. Examples of products to identify are:

(a) Process-related documentation (e.g., plans, standards, procedures).

(b) Requirements.

(c) Design.

(d) Software code units.

(e) Test procedures.

(f) Software system builds for the test activity.

(g) Software system build for delivery to the end user.

(h) Compilers.

(i) Other support tools.

(2) Assigned unique identifiers.

(3) Specified by characteristics.

(4) Specified to a baseline.

(5) Specified to a development phase.

(6) Associated with one person responsible for it, i.e., the owner, from a software CM point of view.

e. Initiate, record, review, approve, and track change requests and problem reports for all configuration items, components, and units according to a documented procedure.

f. Control changes to baselines according to the NCP process for NAS systems or as authorized by the Program Manager for non-NAS systems. Changes processes shall meet the following objectives:

(1) Performance reviews and/or regression tests shall be carried out to ensure that changes have only intended effects on the baseline.

(2) Only configuration items, components, and units which are approved by the software configuration control board are entered into the baseline library.

(3) All configuration items, components, and units are checked in and out of the software baseline library in a manner that maintains the library's correctness and integrity.

g. Generate and control the release of products from the software baseline library according to a documented procedure.

(1) The software configuration control board (CCB) authorizes the generation of products from the baseline library.

(2) Software products from the baseline library, for both internal and external use, are built only from configuration items, components, and units in the library.

h. Record the status of configuration items, components, and units according to a documented procedure.

(1) Recording of software CM actions in sufficient detail so that the content and status of each configuration item, component, and unit are known and previous versions can be recovered.

(2) Maintaining current status and history, i.e., changes and other actions, of each configuration item, component, and unit.

i. Develop standard reports documenting the software CM activities and the contents of the baseline and make the reports available to affected groups and individuals. Examples of reports are:

(1) Software configuration control board meeting minutes.

(2) Change request summary and status.

(3) Trouble report summary and status, including fixes.

(4) Summary of changes made to the software baselines.

(5) Revision history of configuration items, components, and units.

(6) Baseline status.

(7) Results of baseline audits.

j. **Conduct software baseline audits** according to a documented procedure. **Audits** shall:

(1) Assess the integrity of the baselines.

(2) Review the structure and facilities of the software CM library system.

(3) Verify the completeness and correctness of the baseline library contents.

(4) Verify compliance with applicable software CM standards and procedures.

(5) Report the results to the project manager.

6-22. MEASUREMENT AND ANALYSIS.

The Program Manager shall ensure that measurements are made and used to determine the status of the software CM activities. Examples of measurements include:

a. Number of change requests processed per unit time.

b. Number of completed milestones for software CM activities compared to the plan.

c. Work completed, effort expended, and funds expended in the software CM activities.

6-23. VERIFYING IMPLEMENTATION.

The Program Manager shall ensure:

a. **Review of software CM activities with senior management takes place on a periodic basis.** The primary purpose of these periodic reviews is to provide awareness and insight regarding software development activities at an appropriate level of abstraction and in a timely manner. Time between reviews will depend on the effectiveness of mechanisms for exception reporting available. The oversight review addresses:

(1) Technical, cost, staffing, and schedule performance.

(2) Conflicts and issues unresolved at lower levels.

(3) Project risks.

(4) Assignment, review, and tracking of action items until closure.

(5) Summary status report from each meeting that is distributed to affected groups.

b. **Review of software CM activities with the project manager takes place on both a periodic and event-driven basis.** The oversight review shall:

(1) Ensure representation of affected groups.

(2) Review technical, cost, staffing, and schedule performance against the development plan.

(3) Review use of critical resources, against the original estimates.

(4) Identify dependencies between groups.

(5) Raise and resolve conflicts and issues.

(6) Identify project risks.

(7) Assign, review, and track action items closure.

(8) Report summary status to affected groups.

c. **The CM authority** shall carry out periodic audits to verify conformance to documented baselines.

d. **The Program Manager or designated quality assurance individual** shall review and report on activities and work products for software CM.

CHAPTER 7.
DATA COMMUNICATIONS AND NETWORK MANAGEMENT

SECTION 1. GENERAL REQUIREMENTS FOR DATA COMMUNICATIONS AND NETWORK MANAGEMENT

7-1. GENERAL.

a. The communications environment in the FAA includes a wide array of technologies to support local and wide area transport of voice, data and, increasingly, image and video information. The development, operation, and maintenance of a fail-safe communications infrastructure is essential to meeting the FAA's mission of ensuring "the safe and efficient operation of the National Airspace System." Communications and network management in AF shall meet requirements of continuous service in an environment of rapid technological change including implementation of integrated digital networks, LANs and WANs, in a multimedia environment.

b. Planning and operations of telecommunications services within the FAA are carried out by AOP-100 and AOP-200. The AF IRM Division has direct responsibility for the management of interconnectivity for the AF Headquarters LAN and interfaces to the AF wide-area network (WAN). AF must make use of the evolving telecommunications infrastructure and integrate IRM goals and objectives with telecommunications programs. To ensure that AF requirements for data communications in support of administrative data are met, the IRM Division must play an active role in the FAA strategic planning process for telecommunications.

c. The implementation of distributed client-server systems requires that data communications planning and operations must be carefully coordinated with other IRM policies and procedures in such areas as acquisition, data management, configuration management, information systems development, and security. Reciprocally, AF polices and implementation of information systems must be consistent with requirements for network management.

7-2. RELATED PUBLICATIONS.

Other sources that provide more detailed descriptions of data communications and network management procedures include:

a. FAA Telecommunications Strategic Plan, as amended.

b. DOT H 1350.2, Departmental Information Resources Management Manual (DIRMM) Subchapter 8-1, Telecommunications Management Policy.

c. Telecommunications Management and Operations Division (AOP-600), Future FAA Telecommunications Plan (Fuchsia Book), April 1993; Current FAA Telecommunications Plan (Currant Book), Fiscal Year 1991.

d. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 200, National Policy on Controlled Access Protection.

e. DOT 1740.1A, Administrative Telephone Service and Equipment.

f. Airway Facilities Data Communications Strategic Plan (Draft).

g. Government Open Systems Interconnection Profile, FIPS Pub 141.

7-3. AF DATA COMMUNICATIONS AND NETWORK MANAGEMENT OBJECTIVES.

Data communications and network management policies and procedures address the following objectives:

a. Strategic Asset. To develop a strategic plan for AF data communications and

LANs as an asset to benefit all customers and satisfy mission needs.

b. Universal Interoperability. To provide a common network architecture that enables any corporate resource to be accessed transparently by any other resource or user.

c. Network Services. To provide a common set of customer driven network services such as file transfer, electronic mail, directory services, LAN management, server maintenance and security, and distributed network management through a common network environment.

d. Reliability. To maintain uninterrupted operation of critical systems.

e. Uniform Services. To provide customers with a unique ID and with a uniform means for accessing corporate data and network services.

f. User Services. To provide a single organizational point of contact for user services.

g. Integrated Network Management. To provide integrated network and configuration management for data communications and LAN equipment and services.

7-4. DATA COMMUNICATIONS AND NETWORK MANAGEMENT ARCHITECTURE.

The baseline network architecture is a blueprint that defines how critical data communications performance and support requirements are to be met. The architecture includes requirements for the WAN infrastructure and for LAN management. The AF IRM Division shall develop and maintain a baseline architecture for data communications and LANs among AF information systems that is consistent with the FAA telecommunications architecture and standards. The architecture shall:

a. Conform to relevant government, FAA, and industry standards.

b. Provide timely and transparent access, and sufficient data transmission speed, for data communications in a multi-media environment.

c. Provide for a cost-effective migration strategy from existing environments to meet future requirements.

d. Utilize existing and planned FAA telecommunications services.

e. Satisfy NAS and non-NAS data communications requirements.

f. Build a common infrastructure to support data exchange and shared resources, and to facilitate FAA-wide management of corporate data to efficiently support program requirements.

g. Evolve to ensure that data communications facilities and LANs have the capacity to meet AF functional requirements and respond to evolving technology and standards.

h. Define how information resources are being shared, accessed, and managed in an integrated and secure infrastructure.

i. Integrate new technologies as new demands are defined and justified.

j. Meet network and database security requirements. In the case of INTERNET, the FAA shall maintain a single point of entry.

k. Satisfy requirements for disaster recovery to maintain reliability of network operations and access to AF data.

7-5. DATA COMMUNICATIONS AND NETWORK MANAGEMENT REQUIREMENTS.

In order to satisfy the objectives for data communications, AF planning and operations in data communications shall be guided by the following:

a. Multi-year strategic planning processes shall be established for acquiring and operating LANs and other communications facilities that serve data communications requirements to meet program and mission needs. The plan for communications shall be consistent with corresponding plans for related areas such as data management. Plans will be revised annually.

b. Data communications acquisitions shall meet all FAA and AF acquisition requirements.

c. Data communications systems shall be acquired or developed in a way that meets open systems standards and requirements for interoperability and adaptability to new requirements.

d. Data communications systems, including LANs, shall be designed and operated to meet mandated levels of security.

e. Plans shall be developed to maintain reliability and reasonable continuity of support in case the normal operations of data communications systems are disrupted.

f. The AF IRM Division shall mandate the use of FIP and FAA communications standards unless use of accepted standards impedes the agency in accomplishing its mission and a specific waiver is granted.

g. AF IRM plans and procedures for data communications and LANs shall support the AF IRM Functional Plan and the AF Data Communications Strategic Plan.

h. AF shall use appropriate automated systems to conduct and maintain inventories of major network facilities.

i. Where data communications requirements cannot be supported with the existing ADTN facility, AF shall make use of GSA's FTS-2000 network. 800-number services should be employed only when ADTN or FTS-2000 cannot meet the communications need.

7-6. DATA COMMUNICATIONS AND LAN REQUIREMENTS.

a. Acquisition of data communications and LAN equipment and software. New acquisitions of data communications and LAN facilities shall take place only where agency needs cannot be met through interagency sharing of facilities. Data communications systems shall not unnecessarily duplicate systems available from other FAA organizations.

b. Interoperability. Data communications and LAN systems shall be acquired and developed in a competitive manner to minimize life cycle cost and to meet requirements for compatibility, interoperability, and flexibility.

c. Legal requirements for network application access. Data communications capabilities shall support existing legal and regulatory requirements related to data sharing or access. In particular, data communications systems shall respect licensing restrictions for access to network software and applications.

d. Data communications bandwidth. Increases in bandwidth shall be provided to meet demonstrated need in relation to prioritized business requirements. Appropriate justification must accompany requests for data communications services.

e. Network operations. Operational procedures for data communications and networks shall ensure efficient, effective, and secure provision of network services.

f. Back-up and disaster recovery. Plans for back-up and disaster recovery shall maintain reliable service from data communications systems and network servers.

g. Uniform Procedures for Network Access. AF shall implement facilities and establish procedures to provide for uniform access to network services and corporate data for any information systems user in AF.

h. Transparent access to corporate data. The network infrastructure and interfaces to communications facilities shall ensure authorized access to corporate data.

7-7. DATA COMMUNICATIONS AND NETWORK STANDARDS.

a. To achieve interoperability and reduce acquisition costs, AF shall support implementation of DOT, FAA, and FIP standards. Use of appropriate standards shall support the implementation of an OSI environment for data communications. Examples of governing standards include:

(1) NAS Message Transfer Standards (FAA-040/041), which provides for peer-to-peer message transfer.

(2) FAA/AIT Naming and Addressing Standard, which specifies a naming and addressing scheme ensuring uniqueness of addresses.

(3) **Message Priority Standard (FAA-STD-043)**, which enables prioritization of critical messages.

(4) **Directory Services Standard (FAA-STD-044)**, which provides for management of OSI directory information.

(5) **Security Standard (FAA-STD-045)**, which provides requirements for OSI security mechanisms.

(6) **Network and Systems Management Standard (FAA-STD-046)**, which provides for management of fault events, accounting, configuration, and performance within an OSI network.

(7) **Conformance Testing Standard (FAA-STD-047)**, which ensures that vendor development OSI products meet NAS requirements.

(8) **Interoperability Testing Standard (FAA-STD-048)**, which provides for testing of vendor supplied OSI products with respect to NAS interoperability requirements.

b. Standards Implementation. The AF IRM Division shall ensure that requirements and implementation plans for standards are coordinated with designated IRM Representatives, and Program Managers for major systems.

7-8. DATA COMMUNICATIONS AND NETWORK PERFORMANCE REQUIREMENTS.

AF will establish requirements and procedures for monitoring performance of LANs and support for data communications. Performance evaluation requirements shall be established for:

a. Security.

b. Reliability.

c. Accuracy.

d. Utilization.

e. Transparent access to corporate data and network services.

f. Response time for network services, applications, and support.

7-9. SECURITY.

In general data communications for AF facilities can meet lower levels of criticality than communications systems that directly support real-time air traffic data. Nevertheless, AF data communications must support security requirements for data encryption, network access, and password protection for networks and systems that may contain sensitive data. The AF security program for LANs and WANs shall conform to FAA Order 1600.54B and AOP-400 requirements for network security.

7-10. CONFIGURATION MANAGEMENT.

a. Network operations are particularly sensitive to changes in configuration of local hardware and software, which are interfaced to local- and wide-area networks. AF shall support a database that tracks inventory and maintains information on the status and configuration of all equipment connected to AF networks. AF managers shall implement procedures that authorize and monitor changes to network equipment and software. Users shall not make unauthorized changes to local equipment or software, which may affect LAN operations. In addition, users shall coordinate installation of new hardware or software with the LAN manager. A detailed description of CM requirements is provided in Chapter 6.

b. All requests for connectivity to the Headquarters AF network backbone must be approved by the AF IRM Division. All connections to the AF LAN backbone shall meet existing configuration requirements as well as required naming and addressing convention standards.

7-11. OTHER NETWORK MANAGEMENT FUNCTIONS.

a. Network Management Standards. AF information systems shall conform or migrate to AF standards, such as General Network Management Protocol (GNMP), for network management. Managers responsible for information systems maintenance and modification shall implement migration plans to comply with network management standards and procedures.

b. Network Naming and Addressing Conventions. The AF IRM Division shall

implement a standard means for addressing users, servers, and other devices connected to AF networks. The standard employed within AF shall conform to AIT standards as they are developed for WAN and LAN addressing.

c. User Problem Support. AF shall implement procedures for responding quickly and effectively to user requests and problems. In general, each region shall establish a single point of contact to address technical problems with network operations.

d. Network Access. AF shall implement standard procedures for access to network applications and login sequence.

e. Training in Network Applications. Effective training will reduce requirements for problem support. AF shall develop appropriate documentation and training materials and related programs to ensure that users have the knowledge and skills to make use of network services and applications.

f. Software Standards. The AF IRM Division shall establish a common set of software application and version levels to facilitate the exchange of data within AF.

g. Network Applications. The AF IRM Division shall establish network requirements for applications to be installed on AF LANs.

SECTION 2. DATA COMMUNICATIONS MANAGEMENT ROLES AND RESPONSIBILITIES

7-12. GENERAL.

a. The AF IRM Division shall retain overall responsibility for coordinating definition of data communications procedures and other requirements and for monitoring the implementation of AF data communications and LAN requirements within AF. These responsibilities shall be coordinated with AOP-400/600 and AIT strategies and standards for provision of data communications and LAN services.

b. Within their organizations, the AF IRM Representatives for the regions and centers shall be responsible for the implementation of AF data communications and network management procedures and standards, including LAN administration. At Headquarters, because of the complexity of the communications management tasks, there shall be one person responsible for data communications and one person responsible for LAN administration within the AF IRM Division. Finally the Program Managers for major systems shall plan and implement data communications capabilities that are specific requirements of the information systems in their areas of responsibility.

7-13. AF IRM DIVISION RESPONSIBILITIES.

In addition to responsibilities mentioned in Section 1, the AF IRM Division has the following areas of responsibility:

a. Planning and Guidance. As part of its AF IRM planning function, The AF IRM Division shall provide guidance and coordination for planning and shall oversee development of procedures and guidelines for data communications and LANs. Specific areas of responsibility include:

(1) Annual Strategic Plan and Guidance for AF IRM communications facilities and Network Management.

(2) Orders defining guidelines policies, and procedures for data communications and Network Management.

(3) Periodic program assessments.

(4) Migration plans for legacy systems to meet future data communications and LAN requirements.

(5) Strategies and plans for Network Management process improvement.

(6) Business cases for data communications and LAN strategies and programs.

(7) Implementation plans for data communications and network management.

(8) Plans and budgets for NASMAP and related national data communications and network management program resources.

b. Establishment of procedures for:

(1) Access control and security.

(2) Network maintenance.

(3) CM.

(4) Network access.

(5) Network application usage.

(6) Interconnectivity.

c. Providing and administering data communications and LAN administration for FAA Headquarters.

d. Review of data communications and LAN implementation plans in relation to IRM requirements.

e. Maintenance of information on data communications and LAN services, equipment, and configuration.

f. Providing guidance and direction for regional network management.

(1) Design and implementation of AF data communications architecture including interfaces between regional backbones and the FAA WAN.

(2) Monitoring implementation of standards for regional LANs.

g. Monitoring impact of communications and LAN migration plans on other IRM areas such as acquisition data management, security, and information systems development.

h. Establishment of standard procedures to model and track AF data communications and LAN requirements.

i. Selection and implementation of network management standards and automated tools for monitoring data communications and LAN performance.

j. Establishment and monitoring of procedures for data communications and LAN security.

k. Establishment of specific facilities, procedures, and standards to promote data sharing and interoperability among AF systems.

l. Serving as a liaison to other organizations which impact AF data communications and network management.

m. Establishment of procedures for acquiring and implementing Network Management tools.

7-14. AF DESIGNATED IRM REPRESENTATIVE RESPONSIBILITIES.

The designated IRM Representative is responsible for implementation of data communications and LAN management policies and standards within headquarters, the regions, and centers and for evaluating plans for network implementation within regions. Specific areas of responsibility include:

a. Network Management

(1) LAN Administration.

(2) Implementing Network Management policies, procedures, and guidelines.

(3) Evaluating the performance of the networks and recommending enhancements.

(4) Identifying network requirements.

(5) Carrying out program reviews and establishing regional objectives for network management.

(6) Planning and budgeting for network upgrades.

(7) Designing and implementing network changes and improvements.

(8) Providing guidance, support and direction to local organizations on LAN administration and other network concerns.

b. Data Communications Management.

(1) Implementing data communications policies and procedures, guidelines and standards.

(2) Evaluating data communications performance and recommending enhancements.

(3) Identifying data communications requirements.

(4) Carrying out program reviews and establishing regional objectives for data communications.

(5) Planning and budgeting upgrades.

(6) Designing and implementing changes and improvements.

(7) Providing guidance, support and direction to local organizations on data communications.

7-15. RESPONSIBILITIES OF PROGRAM MANAGERS FOR MAJOR SYSTEMS.

a. Program Managers who oversee systems development and operations of major information systems shall ensure that implementation of data communications and network capabilities is consistent with the policies and procedures specified in this order and in related orders and federal regulations. Currently operational communications environments and systems will come into compliance with the order after a reasonable period of transition.

b. Program Managers shall coordinate planning and implementation of data communications and LANs with appropriate designated IRM Representatives and the AF IRM Division. Offices of Primary Responsibility (OPRs) shall ensure that implementations make maximum use of existing data communications facilities and conform to AF and FAA requirements for data communications and LANs.

CHAPTER 8.
AUTOMATED INFORMATION SYSTEMS (AIS) SECURITY

8-1. GENERAL.

The risk of loss, unauthorized use, unauthorized disclosure, loss of integrity, or loss of availability of AF corporate data grows as business becomes increasingly information intensive and as the need to communicate this information on a global scale increases. Preserving the integrity and security of AF data and systems is a corporate effort.

8-2. EXISTING POLICY.

Directives and guidelines in this order supplement existing policy found in the following related publications.

a. DOT H 1350.2, Departmental Information Resources Management Manual (DIRMM), Chapters 4 and 11, Information Systems Security.

b. FAA Order 1600.54B, FAA Automated Information Systems Security Handbook.

c. DOT Order 1640.1C, DOT Computer Security Program (COMPUSEC) Manual.

8-3. SCOPE.

a. Data communications, telecommunications, and automated information processing systems are highly susceptible to interceptions, unauthorized access and exploitation. Protection is needed for proper access by authorized users, denial of unauthorized users, unauthorized disclosure or transfer of data, disclosure of security mechanisms, manipulation, misuse, abuse, and/or deletion of automated information.

b. This chapter establishes Federal Information Processing Resources (FIPR) security principles, concepts, and practices for all AF corporate systems, networks, and data. In the context of this policy, the term security addresses administrative, physical, and technical security for assuring operational reliability.

c. Security is the responsibility of each individual. Security requirements defined within this chapter in other FAA orders apply to all AF personnel. All Program Managers, LAN Administrators, and designated IRM Representatives shall apply a comprehensive and coordinated approach to protect AF corporate information resources.

8-4. ROLES AND RESPONSIBILITIES.

a. The National AIS Security Program Manager is the focal point for all security matters for the FAA. See FAA Order 1600.54B, paragraph 10.

b. Program Managers for major systems shall oversee and implement required security procedures in their respective programs.

c. The Automated Information Systems Security Officer (AISSO) is responsible for security oversight within a designated organization.

d. The AF IRM Division supports the implementation of AIS security requirements of the Office of Civil Aviation Security. The AF IRM Division also monitors policy implementation with respect to AF corporate systems, networks, and data.

e. Designated IRM Representatives monitor implementation of security procedures for their areas of responsibility. The designated IRM Representatives shall support all DOT and FAA security policy and procedures by reviewing, monitoring, and auditing established security practices in their respective areas of responsibility.

f. The designated AF IRM Representative for Headquarters is responsible for headquarters security. The headquarters IRM Representative shall coordinate AF IRM security practices with the National AIS Security Program Manager.

g. Designated IRM Representatives shall also provide for security awareness training.

h. **Other FAA security** roles are described in FAA Order 1600.54B, paragraph 10.

8-5. OBJECTIVES.

The AF IRM Division's objectives in defining a security discipline for AF corporate systems, networks, and data are to:

a. Identify the systems, networks, and data that are critical to AF mission.

b. Implement security programs as appropriate to the criticality and/or sensitivity of data.

c. Evaluate each personal computer and LAN environment to ensure that the level of security implemented agrees with the value and sensitivity of data residing on information systems.

d. Ensure that personal computers are in compliance with existing policies and standards.

e. Ensure that appropriate security measures are implemented for system development activities.

f. Address identified threats and vulnerabilities.

8-6. ADMINISTRATIVE SECURITY.

The respective Program Manager, Regional Manager, and LAN Administrator shall ensure that:

a. Systems within their domain are properly classified.

b. Effective measures are put in place to ensure continued operations and processing of mission-critical systems during emergency situations.

c. Measures are established to ensure the protection of mission-critical systems, networks, and data and mitigate vulnerabilities.

d. Guidelines are developed for software evaluation and assigning appropriate authority to personnel for each installation.

e. Data is available to authorized employees, contractors, and users who have a valid need for it.

f. All security violations, or suspected violations, are immediately reported to the AISSO.

8-7. PHYSICAL SECURITY.

a. The designated IRM Representative shall perform on-site visits to inspect installations for enforcement and practice of established procedures. When necessary, the designated IRM Representative shall make recommendations for improvements, e.g., cipher locks, card key entry systems, sign-in/sign-out logs, visitor control procedures, etc.

b. Reasonable measures shall be used to secure all computer equipment and comply with physical security requirements as specified in FAA Order 1600.54B.

c. The borrower/user of government hardware and software shall report its loss, theft, and damage immediately to the AISSO.

8-8. TECHNICAL SECURITY.

The respective Program Manager, Regional Manager, and LAN Administrator shall ensure that:

a. In addition to the password protection policy in FAA Order 1600.54B, paragraphs 406 and 909, AF employees shall change their password every 90 days or immediately if password-protected access is compromised. The AISSO must change the user's password in response to a change in a user's access authority.

b. Data stored on network servers shall be backed up on a regular basis and stored in accordance with FAA security requirements.

8-9. SOFTWARE.

a. Non-commercial, proprietary software shall be considered sensitive. Proprietary software shall be controlled in accordance with the security plan of the system which uses it.

b. All AF employees shall use only appropriately acquired and licensed software on government-owned systems. See Chapter 6, Configuration Management, for requirements regarding licensing.

c. The designated IRM Representative shall provide guidance on the use of specific public domain programs and utilities.

8-10. PERSONAL HARDWARE AND SOFTWARE IN THE WORKPLACE

Individual user responsibility for privately owned hardware and software is found in FAA Order 1600.54B, paragraph 911. All personal hardware and software shall be brought into the workplace at the risk of the owner. The government bears no liability for privately owned hardware and software as stated in FAA Order 1600.54B, Chapter 9. All privately-owned hardware and software may be subject to automated audits and/or other monitoring procedures for compliance with license agreements. The user of the system must hold a valid license for hardware and/or software.

8-11. DISASTER RECOVERY.

Procedures for contingency planning and disaster recovery shall meet requirements specified in FAA Order 1600.54B, paragraph 384 and Chapter 10.

a. **AF Corporate Data.** All data related to FAA business functions shall be stored and backed-up in accordance with FAA Order 1600.54B requirements.

b. **Data on AF Networks.** Data stored on network servers shall be backed-up regularly, depending on volatility and criticality of the information, and stored in accordance with FAA security requirements.

8-12. PORTABLE COMPUTERS.

In addition to the policy stated in FAA Order 1600.54B, paragraph 324, the borrower/user of a portable computer shall:

a. Not check the computer as baggage unless it is properly marked and properly packed in a shipping carton.

b. Report its loss, theft, or damage immediately to the AISSO.

8-13. VIRUS REMEDIATION.

a. Designated IRM Representatives shall establish a virus remediation program in their local areas to identify, eradicate, and prevent computer viruses. The designated IRM Representative shall provide the most current version of the virus re-mediation software to all users.

b. Program Managers for major systems and LAN Administrators of mission-critical systems and networks shall run virus checking software daily to alert the AISSO of the presence of possible viruses. If a virus is discovered or suspected, the AISSO shall be notified immediately, and the program manager or LAN administrator shall take prompt action to control and eradicate the surreptitious code and correct any damage or loss that may have occurred. It is recommended that the virus software run as a Terminate and Stay Resident (TSR) program for DOS-based systems, or a a Virtual Device Driver (VDD) for Windows-based systems, in order to continually check for the introduction of a virus. Virus software shall be run before every backup on AF networks and workstations. Program managers and/or LAN administrators shall run virus-checking software at least once a week.

8-14. AWARENESS TRAINING.

Designated IRM Representatives shall ensure there are appropriate training programs in place in their respective areas concerning security awareness and accepted computer practices.

8-15. THREAT ASSESSMENT.

See FAA Order 1600.54B, paragraph 203, Chapter 11, and Appendix 3 on risk analysis. A risk analysis shall be completed periodically at the discretion of the designated IRM Representative on all AF corporate systems, networks, and data in their respective areas.

CHAPTER 9. INFORMATION SYSTEMS DEVELOPMENT AND MAINTENANCE

SECTION 1. GENERAL DEVELOPMENT INFORMATION

9-1. GENERAL.

a. The planning, design, development, and implementation of automated information systems and applications absorbs a large amount of human, financial, and FIP equipment resources within the FAA. The FAA is committed to improving the process of systems development in order to enable information systems to meet mission requirements, and at the same time, reduce the time and costs associated with systems development and maintenance. AF will support FAA initiatives in software modernization including use of Computer-Aided Software Engineering (CASE) tools, software-related standards, and development of repositories for software products.

b. A defined process for system development and decision-making is needed at each stage of the development life cycle to maximize the return on this investment and to provide for cost-effective operation, revision, and maintenance. The ISD process must be integrated with other processes and requirements that support planning, acquisitions, AIS security, and data communications services.

c. This section provides guidance for AF implementation of a common process for in-house development of AF corporate systems. The objective is to build upon standard processes such as those defined in FAA STD-026. Such standards have already been used in the development of AF systems such as the Maintenance Management System (MMS) program.

d. Directives and guidelines within this chapter are based on principles and guidelines for systems and software development developed by the Software Engineering Institute and the Information Systems Development (ISD) Manual developed at the Volpe National Transportation Systems Center. The described ISD process defines four types of life cycles to support the varying levels of complexity of development efforts within AF.

9-2. APPLICABILITY.

This chapter applies to all AF corporate system development projects, including major enhancements of existing systems. The term "system" refers to both system and software development. Currently operational systems or systems under development prior to the approval of the AF IRM Order will be expected to comply with the order after a reasonable period of transition. All system development projects shall meet the following requirements:

a. The Program Manager for the information system shall submit the project to the AF IRM Division for inclusion in AF system inventories. All relevant AF organizations shall have an opportunity to review the system requirements for possible impact on their organizations.

b. All systems under consideration for development shall be reviewed with respect to the corporate IRM needs of the FAA. Wherever possible, systems, and resident data, will serve more than one organization or purpose.

c. Planned system development activities shall be coordinated with the designated IRM Representative, ASU (Contracts and Quality Assurance) and/or ALM (Life Cycle Management), as appropriate.

9-3. INFORMATION SYSTEM INITIATION AND BUSINESS PROCESS IMPROVEMENT.

The identification of requirements and development of new information systems applications must follow from analysis of opportunities to improve business processes. Evaluation, development, and implementation

of new information systems and modification of existing information systems should be carried out with the primary objective of facilitating changes in business processes that more effectively and efficiently meet mission requirements. Further information on required justification and review of new information systems is given in Chapter 4.

9-4. STANDARDS AND POLICIES.

The following publications provide guidance for ISD projects:

a. Project Initiation.

(1) FIPS Publication 64, Guidelines for Documentation of Computer Programs and Automated Data Systems.

(2) FAA Order 1370.52C, Information Resources Management — Policies and Procedures, Chapter 5.

b. System Development and Maintenance. Military Standard Defense System Software Development, FAA STD-026. This standard establishes uniform requirements for software development that are applicable throughout the system life cycle.

c. Quality Assurance (QA). Development and implementation of information systems shall employ appropriate quality assurance methods. Standards for QA are defined in:

(1) FAA-STD-013, Quality Control Program Requirements.

(2) FAA-STD-016, Quality Control System Requirements.

(3) FAA-STD-018, Computer Software Quality Program Requirements.

(4) FAA-STD-016, Quality Control System Requirements.

(5) FAA Order 4453.1B, Quality Assurance of Material Procured by FAA.

9-5. PROJECT INITIATION AND DOCUMENTATION.

As outlined in Chapter 4 of this order and in FAA Order 1370.52C, the initiation of a new systems development project or major modification must demonstrate the need for new functionality in relation to mission need and the unavailability of alternative means for satisfying mission requirements. Following acceptance of a project request, the Program Manager shall carry out formal analysis of system requirements and alternatives. The resulting documentation includes:

a. Requirements Analysis. This document includes a statement of mission need. The analysis considers:

(1) Information processing functions to be performed.

(2) Identification and location of related FAA applications systems and software.

(3) Nature of data to be generated, who will maintain it, and who will require access to the system.

(4) Consideration of alternative means of meeting stated functional requirements.

(5) Expected benefits of system implementation.

(6) Space management requirements.

(7) Present and projected workload.

(8) Performance evaluation of the current system.

(9) A comparison of the risk of acquiring insufficient FIP equipment capacity versus the risk of assuming extra costs by acquiring excessive capacity; and performance validation techniques to be used in any related acquisitions (FIRMR 201-30.007). Other acquisition-related considerations include justification requests for waivers from specific IRM requirements and use of full and open competition (FIRMR 201-30.009-3).

b. Analysis of Alternatives. This includes a comparative cost analysis of alternative methods of fulfilling the user's requirements and encompasses, at a minimum:

(1) Consideration of use of non-FIP resources.

(2) Use of existing facilities.

(3) Use of commercial facilities.

(4) Redesign of application programs.

(5) Production schedule revision or work shift revisions.

(6) Augmentation, upgrading, or replacement of a FIP system or components (FIRMR 201-30.009).

(7) Identification of project management roles and responsibilities. Additional management requirements are provided in FAA Order 1370.68, Automated Data Processing Information Technology Facility (Host Resource) Selection.

c. **Management Decision Paper.** The project analysis and analysis of alternatives as well as related documentation are summarized in the Management Decision Paper. This paper shall also present a plan of action for the remaining steps of the development life cycle along with a project management plan. Upon completion:

(1) The Management Decision Paper, supported by the other two documents, is sent through the appropriate IRM to the AF IRM Division for review with respect to IRM requirements.

(2) If the costs, benefits, and schedules for project completion are within the parameters approved in the AF IRM plans and no substantial problems are identified by the AF IRM Division or other review organizations, the Program Manager will implement the action plan contained in the Management Decision Paper.

(3) Upon approval by required levels of acquisition review, the Program Manager shall implement the project management plan.

9-6. OPEN SYSTEM ARCHITECTURE.

To promote interoperability, new system development efforts should utilize an open system architecture and avoid use of proprietary hardware and operating systems. Refer to FIPS PUB 146-1, Government Open Systems Interconnection Profile (GOSIP) for guidance.

9-7. MIGRATION OF LOCAL SYSTEMS AND APPLICATIONS TO AF CORPORATE SCOPE.

When a local system or local software is designated by a program office in conjunction with the AF IRM Division review as an AF corporate system, it shall be treated in status as an AF corporate system. The Program Manager will assign a data systems manager. Once a system is designated as AF corporate, all the system development processes described in this chapter shall be reviewed for applicability under the new status. In addition, the Program Manager shall ensure the development of adequate documentation and configuration management of the system as stated in this order.

SECTION 2. IN-HOUSE SYSTEM DEVELOPMENT PROCESS

9-8. SYSTEM DEVELOPMENT LIFE CYCLES.

a. The Program Manager shall select and oversee the application of one of the three AF life cycles to develop AF corporate information systems. Two life cycles involve a structured, top-down approach (one for more complex systems, one for less complex systems). The other life cycle uses an evolutionary approach involving an iterative process resulting in the development of one or more prototypes that provide increasing levels of functionality required of the completed operational system. The use of prototypes to assess system functionality in relation to user requirements is encouraged in all three development processes.

b. The process of system and software development is outlined in Appendix 1, FAA Airway Facilities (AAF) Information Systems Development (ISD) Handbook. It is based on the DOD 2167A standard, tailored to the three life cycles. Determinants in the selection of a life cycle involve the size, complexity, and

degrees of business and technological change brought on by building or implementing the system. (See the ISD Handbook for a description of the life cycles' project characteristics, management skills needed, and other general issues.) The life cycles are:

(1) Structured Development Life Cycle: The Program Manager shall use this life cycle for a project that involves:

(a) Low business change.

(b) High technological change.

(2) Limited Structured Development Life Cycle. The Program Manager shall use this life cycle for a project that involves:

(a) Low business change.

(b) Low technological change.

(3) Evolutionary Development Life Cycle. The Program Manager shall use this life cycle for a project that involves:

(a) High business change.

(b) High technological change.

c. There is a fourth type of development, designated "limited-evolutionary." This type is used when there is a high business change and low technological change. It is characterized by a difficult business problem, that once solved, is easy to implement (e.g., through a spreadsheet). No formal development life cycle is required for this type of development.

d. Figure 9-1 illustrates the life cycle selection guidelines. Figure 9-2 illustrates the conceptual differences in the structured and evolutionary processes.

9-9. LIFE CYCLE PHASES AND ACTIVITIES.

a. The following phases of system development are the same in all three life cycles. The Program Manager shall employ all six phases in AF development projects.

(1) System Requirements Analysis & System Design.

(2) Software Requirements Analysis.

(3) Design.

(4) Code and Test.

(5) System Acceptance Testing.

(6) Implementation and Evaluation.

b. The phase names are consistent across life cycles. Each phase has a certain set of activities involved. The activities and their timing depend upon the life cycle selected. See Appendix 1 for the full list of activities within each phase. Appendices 2, 3 and 4 are checklists of all possible activities that can be undertaken during each development life cycle. Respectively, they are, the structured, the limited-structured, and the evolutionary-development life cycles.

c. The Program Manager shall ensure the project management plan coincides with the phase activities of the chosen life cycle. A baseline results from the initial completion of the requirements analysis or system design. Each major activity or phase results in a newly defined baseline of the system. Baselines can be altered only through accepted change control processes (see Chapter 6 of this order). The Program Manager shall use appropriate, and preferably standard, project management tools to control and report on the state of the phased development effort and monitor the contractor development process.

FIGURE 9-1. CHANGE ASSESSMENT MATRIX

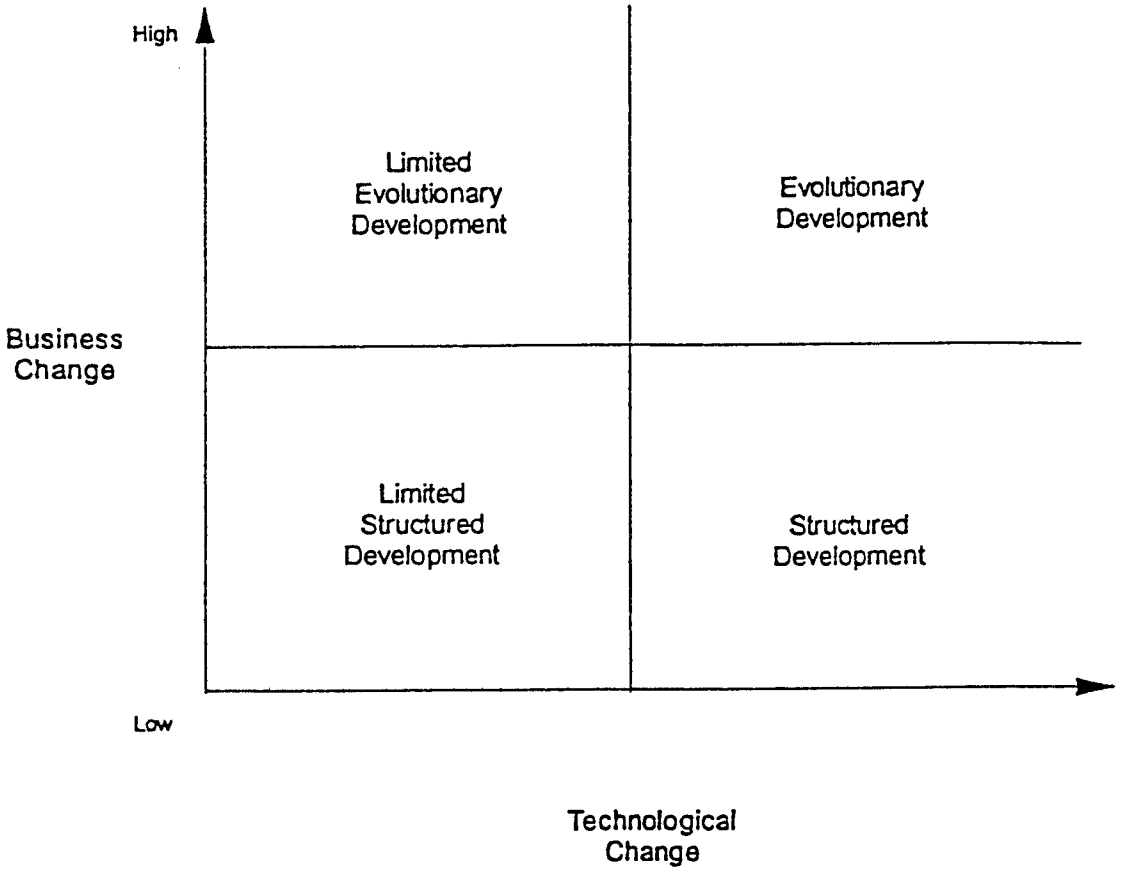
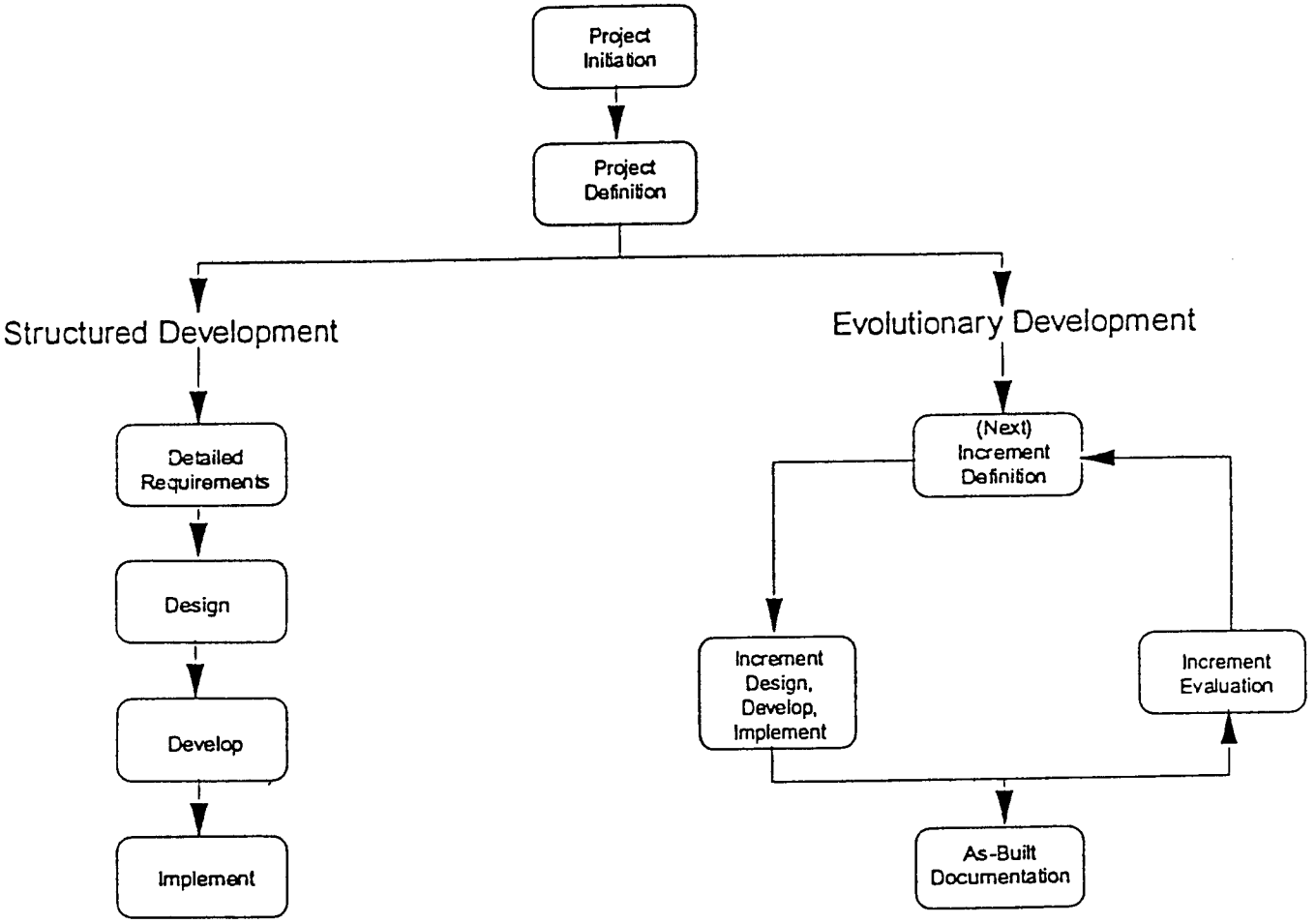


FIGURE 9-2. STRUCTURED AND EVOLUTIONARY PROCESSES



9-10. SELECTING A SYSTEM DEVELOPMENT LIFE CYCLE.

The Program Manager shall select a life cycle model that is most appropriate to the level of change in business and technology associated with the project. (See the evaluation procedure described in Appendix 5).

9-11. TAILORING THE STANDARDS.

The FIPS PUB 64 and DOD-2167A standards selected represent the most detailed set of activities and associated documentation to support system development. DOD 2167A can be tailored to meet AF requirements for life cycle management. The Program Manager shall ensure that tailored requirements continue to ensure the quality of computer hardware, software, and associated documentation delivered as part of the system.

9-12. BASELINES.

Baselines provide AF with a means for monitoring development progress, determining configuration status, and evaluating quality of each work product. (See Chapter 6, section 2 of this order for more detail on configuration management requirements.)

9-13. TRAINING.

The Program Manager shall ensure that project staff members receive appropriate training in estimating, scheduling, the commitment process, development standards, life cycles, and change management.

9-14. CHANGE PROPOSALS - REVIEW AND APPROVAL.

Upon receipt of the FAA Form 1370-18, Data System Change Proposal, the Program Manager or the data systems manager will assign a sequential number to it and coordinate the change with affected office(s) and the appropriate IRM to determine if it represents a valid change. In the event the AF corporate information system is operating without an approved data dictionary, the manager should also send copies of the Data System Change Proposal to the AF IRM Division.

9-15. INFORMATION SYSTEMS MAINTENANCE.

For system enhancements, the levels of change to business and technology will determine the appropriate life cycle. Based on the impact of the change to the existing system, a reduced life cycle may be appropriate. For example, a simple change may have no effect on the design. For more significant changes to a system, the Program Manager shall develop a Project Management Plan, which specifies the activities for each required phase.

9-16. PROCESS MANAGEMENT.

In order for the system development process to be versatile and meet future requirements, AF Program Managers shall participate in the continued definition, execution, analysis, and control of the development process. The AAF ISD Handbook in Appendix 1 shall be updated by the AF IRM Division as new requirements and opportunities for improving the development process are identified.

SECTION 3. CONTRACT SYSTEM DEVELOPMENT

9-17. SOFTWARE QUALITY ASSURANCE.

The Program Manager shall ensure that contractors have a Software Quality Assurance (SQA) process to support AF system development efforts. The Program Manager shall ensure that the SQA principles and guidelines outlined in Appendix 6, Software Quality Assurance are applied throughout the development life cycle. The Program Manager shall contact ASU-400 for planning the required SQA support for major systems.

9-18. CONTRACTOR REQUIREMENTS.

The Program Manager shall ensure that contractors developing AF corporate systems follow the guidelines in Appendix 7, AF Contractor Requirements. The Program Manager shall:

a. Establish requirements for the contractor's software maturity level as defined by the Software Engineering Institute (SEI).

(1) As with in-house development efforts, the use of a well-defined process, in accordance with SEI maturity specifications, can improve performance of software development tasks.

(2) The contractor's software process maturity level (SEI rating) can be used as a guideline to gauge the risk involved in using a particular contractor. It takes most organizations several years to move from one level to another. It is expected that AF contractors have a plan to achieve at least a level-three capability.

b. Specify control requirements before development. The Program Manager shall:

(1) Completely specify all requirements for technical performance , cost, schedule, and data rights.

(2) Establish methods for monitoring the contractor's progress.

(3) Establish methods for accepting and controlling changes to the contractor's products. The contractor is normally required to establish a change control board which interacts with AF's change control board (if applicable). The contractor's methods for change control shall be described in the contractor's software configuration management plan.

APPENDIX 1. FAA AIRWAY FACILITIES INFORMATION SYSTEMS DEVELOPMENT (ISD) HANDBOOK FOR SYSTEM DEVELOPMENT PROJECTS

What is the ISD Handbook?

The Information Systems Development (ISD) handbook presents a process which is a set of preferred ways for conducting the business of developing an information system. It is based on DOD-STD-2167A, Military Standard Defense System Software Development, in that DOD 2167A is integrated throughout each of the three development life cycles within the handbook. DOD 2167A specifies what steps should be taken in developing software and this handbook provides the underlying procedure that supports the successful completion of each step.

Who Should Use the ISD Process?

Anyone initiating, defining, developing, or overseeing system development of information systems for AF corporate systems.

Value/Benefits of the ISD Process

- Industry proven guidance in developing successful information systems
- Less risk with project schedules and resources
- Successful handling of impact of business change on information systems
- Promotion of common understanding through a common vocabulary and process
- Choice of methodology, tools

What is the Basis of the ISD Process?

- Most recent industry accepted software development models.
- Applicability to nearly all types of information systems projects.

What Does the ISD Process Consist of?

- There are six phases for information systems:
  - + Phase 1: System Requirements Analysis & System Design
  - + Phase 2: Software Requirements Analysis
  - + Phase 3: Design
  - + Phase 4: Code and Test
  - + Phase 5: System Acceptance Testing
  - + Phase 6: Implementation and Evaluation

- There are three development life cycle models for the process:
  1. Structured Development Life Cycle
  2. Limited Structured Development Life Cycle
  3. Evolutionary Development Life Cycle

- There are rationales to help determine the choice of models, based upon both business and technical considerations (see paragraph 9-10 and Appendix 5 of the AF IRM Order)

- Activities and products for each of the six phases within a model are specified:
  - Entrance criteria
  - Exit criteria
  - Documents
  - Reviews
  - Activities.

- There is consideration for the integration of business change with information systems development.

What's First?

- Follow the Project Implementation Plan (PIP).
- Review the life cycle model chosen for the project.
- Tailor the standards to the project.
- Formalize all tailoring:
  - Update standard forms of documents and reviews, as needed.
  - Update the System Development Plan to reflect the tailoring changes.
- Continue with the selected life cycle.

Items Common to All Life Cycles

- Phase structure: Each life cycle model has the same phase structure containing all six phases.
- Documents, reviews, activities:
  - At each phase of development, certain documents, reviews, and activities are necessary.
  - Each phase within a life cycle has its own requirements for them.
  - All documents, reviews, and activities, as tailored, must be performed.
  - Further tailoring may be done, as the project matures and there is more insight into the project.
  - Documentation and reviews monitor/control the project and manage risk.
  - Management must be assured that all the requirements for documents, reviews, and activities have been met for each phase.

- Entrance and exit criteria for each phase of a life cycle:
  - Criteria for each phase must be completed before continuing with the next phase.
  - Each life cycle has its own criteria (see individual life cycles).

- Incremental and concurrent development:
  - Allows development in more manageable pieces.
  - Incremental development:
    + Critical components are developed and implemented first.

    + Less critical components are developed and implemented in increments later.
  - Concurrent development - Two or more components are developed at the same time.

- Phase feedback (waterfall effect):
  - As development progresses, revisions may be needed in earlier phases:
    + Revisions one level back (without returning) to previous phase's products:
      - Changes must be under configuration management.
      - Discuss changes and come to agreement with the customer.
      - There is no need to repeat the phase's activities.
    + Return to a previous phase's activities (one or more levels back):
      - Changes must be under configuration management.
      - Discuss changes and come to agreement with the customer.
      - Repeat or step through phase's activities.
      - Repeat exit criteria for the phase.

Structured Development Life Cycle

This life cycle model is a derivation of the traditional software development "waterfall" process model.

Characteristics of a project using this model:

- Low business change effect and high technological challenge
- Stable and well understood requirements
- Large systems with many interfaces
- Heavy user involvement
- Formal development environment.

Management skills needed:

- Strong administration skills
- Strong team-building and integration skills
- Ability to keep the team productive and "by the book"
- Ability to see the "big picture" and yet grasp details
- Formal communication with sponsors of work or users of software
- Ability to interpret standards for the project
- Ability to tailor the project appropriately.

General issues:

- Prototyping:
  + A problem may be investigated with prototyping until the problem is resolved.
  + All exit criteria must be met before leaving a phase.
  + Usually there is little prototyping necessary with this model.
- Decomposition and integration:
  + The SDLC model system is decomposed into manageable units (Computer Software Configuration Items (CSCI), Computer Software Components(CSC), Computer Software Units (CSU)) for development and integrated for testing and acceptance.

- Incremental and concurrent development:
  + Begins only after the high level system design and high level software design are complete (System Requirements Analysis and Design Phase).
  + Phase requirements must be followed for each increment or concurrent activity.
- Testing:
  + Helps to manage risk factors.
  + Testing activities are performed at every phase.
  + Testing links to developmental levels of phases, to verify/validate requirements, at the CSU, CSC, and CSCI levels.
  + Testing results are documented.

Phases 1 through 6:

- Characteristics:
  + Each phase is performed sequentially.
  + A phase may be revisited as development progresses.
  + Prototyping may take place in any phase.
  + Prototypes are more than likely discarded.

Phase 1: System Requirements Analysis & System Design:

- System Requirements Analysis:
  + Review high level system requirements and develop them (preliminary requirements).
  + Document the requirements.
- System Design:
  + Segment system between hardware, firmware, and software (CSCIs, Hardware Configuration Items (HWCIs) components and manual operations.
  + Define interfaces.
  + Allocate system requirements to components.
  + Begin decomposition of the system.
  + Update preliminary requirements (still preliminary and high level).
  + Perform planning activities (Software Development Plan):
    - Identify/define standards.
    - Develop project schedule.
    - Define project organization and responsibilities.
    - Define Software Quality Assurance and Configuration Management Plans.
    - Address security issues.
- Exit criteria:
  + Specification documents
  + System Requirements Review
  + System Design Review.
- Upon completion and concurrence by the customer:
  + The functional baseline is established (System Segment Specification (SSS)).
  + Products are placed under configuration management.

Phase 2: Software Requirements Analysis:

- Develop the preliminary requirements further and specify external design (detailed software and interface requirements).
- Prototyping is very useful here.
- Incremental and concurrent development may begin.
- Exit criteria:
  + Requirements analysis documents
  + Software Requirements Review.
- Upon completion and concurrence by the customer:
  + Allocated baseline is established (Software Requirements Specification (SRS)).
  + Products are placed under configuration management.

Phase 3: Design:

- Define internal design of system.
- Preliminary Design:
  + Define subsystem at program level (CSCs).
  + Prove design components (prototype) which are risky.
  + Return to previous phases, if necessary.
  + Begin Project Implementation Plan, with user involvement, and Training Plan.
  + Define the Test Plan.
- Detail Design:
  + Decompose the subsystem to its lowest units (CSUs).
  + Provide enough technical detail to code.
  + Define test cases.
  + Start User and Operations Manuals, and training material.
- Exit criteria:
  + Design documentation
  + Preliminary Design Review
  + Critical Design Review.
- Upon completion and concurrence by the customer:
  + Design specifications are placed under developmental configuration management.

Phase 4: Code and Test:

- Develop test procedures.
- Build and test CSUs, CSCs, to reach CSCI level.
- Make necessary changes to Software Design Document (SDD), modify code, and re-test.
- "Practice" test CSCI.
- Exit criteria:
  + Updated design documentation.
  + Test Readiness Review.
- Upon completion and concurrence by customer:
  + Code, listings, and documentation are placed under developmental configuration management.

Phase 5: System Acceptance Testing:

- Concurrent development efforts meet and merge.
- Integrate procured hardware, software, firmware with developed software.
- Support user in developing test plans, cases, procedures.
- Merge and test all subsystem components (CSCIs, HWCIs).
- Test system as a whole (Configuration Item (CI)).
- Make necessary changes to design or code; re-test and update documentation.
- Prepare Software Product Specification, Version Description Document.
- Support the customer's functional audit.
- Deliver source code and documentation.
- Exit criteria:
  + Updated documentation
  + Formal Qualification Test Review
  + Functional Configuration Audit
  + Physical Configuration Audit.
- Upon completion and concurrence by the customer:
  + A product baseline is established.
  + The system is now fully operational.

Phase 6: Implementation and Evaluation:

- Follow the implementation and training plans.
- Move the fully tested system to operational status.
- The customer evaluates the installed system in the operational environment.
- Provide support to the customer to evaluate system performance.
- Make necessary changes to previous products and recycle through the Structured Development Life Cycle model.
- Exit criteria:
  + Defined by the transition plan
  + Final meeting with the customer for concurrence.
- Upon meeting criteria:
  + The system is now in production
  + The system has maintenance status.
- Deliver all documents.
- Perform training.

Key issues:

- Early implementation planning
- Managing risk - reviews, formal concurrence
- Prototyping for critical components
- Completion of phases - must follow entrance and exit criteria.
- Attention to baselines, configuration management, critical milestones.

Limited Structured Development Life Cycle

This is a scaled-down version of the Structured Development Life Cycle. It is also a derivation of the traditional software development "waterfall" process model.

Characteristics of the project:

- Low business change effect and low technological challenge
- Requirements are stable and well understood
- Involves a single system or a subsystem being built to enhance an existing system. System design and development is not a consideration.
- No system hardware is to be designed or built
- User involvement is likely to be reduced
- The development environment is less formal
- Calls for a limited set of activities, documents, and reviews from the Structured Development Life Cycle.

Management skills needed:

- Comfortable working in an informal environment
- Able to provide direction and guidance to a small team
- Able to contribute technically as an individual
- Can interpret standards for the project
- Can tailor the project appropriately.

General issues:

- Decomposition and integration:
  - + The Limited Structured Development Life Cycle model system is decomposed into manageable units (CSCI, CSCs, CSUs) for development and integrated for testing and acceptance.
  - + Decomposition is simpler than the full Structured Development Life Cycle - no CIs.
- Testing:
  - + Helps to manage risk factors.
  - + Testing activities are performed at every phase.
  - + Testing links to developmental levels of phases, to verify/validate requirements, at the CSU, CSC, and CSCI levels.
  - + Testing links are simpler than the full Structured Development Life Cycle (no CIs).
  - + Testing results are documented.
- Prototyping:
  - + A problem may be investigated with prototyping until the problem is resolved.
  - + The design process should aim to incorporate as much code as possible from the prototype into the final system.
  - + Phases are still performed sequentially.
  - + A phase cannot be exited until exit criteria are met.
- Incremental and concurrent development:
  - + Components are defined during the Design Phase.
  - + Critical components are developed first.

+ Less critical components are developed in increments.
+ Concurrent development involves developing two or more pieces at the same time.
+ Phase requirements must be followed for each increment or concurrent activity.

Phases 1 through 6:

- Characteristics:
  + Each phase is performed sequentially, for the most part.
  + A phase may be revisited as development progresses.
  + Prototyping may take place in any phase.
  + Prototypes are more than likely discarded.

Phase 1: System Requirements Analysis & System Design:

- System Requirements Analysis:
  + Review high level system requirements and develop them (preliminary requirements).
  + Document requirements.
- System Design:
  + Segment the system between hardware, firmware, and software (CSCIs, HWCIs) components and manual operations.
  + Define interfaces.
  + Allocate system requirements to components and begin decomposition of the system.
  + Update preliminary requirements (still preliminary).
  + Perform planning activities (Software Development Plan):
    - Identify/define standards.
    - Develop the project schedule.
    - Define the project organization and responsibilities.
    - Define Quality Assurance and Configuration Management Plans.
    - Address security issues.
  + Procured hardware, software, firmware exit the Limited Software Development Life Cycle, to merge later, in Phase 6.
- Exit criteria:
  + Two documents
  + No reviews, but concurrence with the customer.

Phase 2: Software Requirements Analysis:

- Specify detailed software and interface requirements (complete the preliminary requirements).
- Incremental and concurrent development may begin.
- Define subsystems further, resulting in external design.
- Design includes all user interface requirements and other external interface requirements.
- Prototyping is especially helpful with external design.
- Exit criteria:
  + One document
  + Updates to previous documents
  + Software Requirements Review.

- Upon completion and concurrence by the customer:
  + The functional baseline is established (SRS).
  + Products are placed under configuration management.

Phase 3: Design:

- Define internal design.
- Preliminary Design:
  + Prove design components (prototype) which are risky.
  + Return to previous phases, if necessary.
  + Design external interfaces.
  + Begin design of the physical data base.
  + Begin the Implementation Plan, with user involvement, and Training Plan, using the Project Management Plan
  + Define the Test Plan.
- Detail Design:
  + Decompose the subsystem to the lowest units (CSUs).
  + Provide enough technical detail to code.
  + Finish physical data base.
  + Define test cases.
- Exit criteria:
  + Six documents
  + Updates of previous documents
  + Design Review
  + Critical Design Review (optional).
- Upon completion and concurrence by the customer:
  + Design specifications are placed under developmental configuration management.

Phase 4: Code and Test:

- Develop test procedures.
- Integrate and test CSUs, CSCs, to reach CSCI level.
- Make necessary changes to Software Design Document, modify code, and re-test.
- Develop CSCI test procedures.
- "Practice" test CSCI.
- Record all test results.
- Integrate procured hardware, software, firmware with developed software, if available.
- Exit criteria:
  + Ongoing documents
  + Updated documents
  + Test Readiness Review.
- Upon completion and concurrence by the customer:
  + Code, listings, and documentation are placed under developmental configuration management.
  + The formal test baseline is established.
  + The system is ready for acceptance testing.

Phase 5: System Acceptance Testing:

- Concurrent development efforts meet and merge.
- Integrate procured hardware, software, firmware with developed software into user's operational environment.
- Support the user in developing test plans, cases, procedures for final test.
- Merge and test all subsystem components (CSCIs, HWCIs).
- Test the system as a whole (CI).
- Report all test results.
- Make necessary changes to design or code; re-test and update documentation.
- Support the customer's functional audit.
- Deliver source code and documentation.
- Exit criteria:
  + Five final documents
  + Updates of previous documents
  + Formal Qualification Test Review.
- Upon completion and concurrence by the customer:
  + A product baseline is established.
  + The system is now fully operational.

Phase 6: Implementation and Evaluation:

- Follow the Implementation and Training Plans.
- Set up a "production" configuration management control system.
- Move the fully tested system to operational status.
- If enhancing an existing system, merge the new system into the operational configuration of the existing system.
- The customer evaluates the installed system in the operational environment.
- Provide support to the customer to evaluate the system performance.
- Make necessary changes to previous products and recycle through the Limited Structured Development Life Cycle model.
- Exit criteria:
  + Defined by the transition plan
  + Final meeting with the customer for concurrence.
- Upon meeting criteria:
  + The system is now in production.
  + The system has maintenance status.
- Deliver all documents
- Perform training.

Key issues:

- Managing risk - reviews
- Completion of phases - must follow entrance and exit criteria
- Prototyping for critical components
- Attention to baselines, configuration management, critical milestones.

Evolutionary Development Life Cycle

Characteristics of the project:

- High business change effect and high technological challenge
- High degree of risk and uncertainty
- Initially, requirements not fully known, or unstable
- Rapid prototyping approach
- Working model develops into a final, deliverable, production system.

Management skills needed:

- Able to work well with business managers and help solve business problems
- Be familiar and effective with the evolutionary approach
- Be an active contributor to the process to translate visions into reality
- Be broad-minded and open to new ways
- Able to interpret standards for the project
- Able to tailor the project appropriately.

Documents, reviews, activities:

- All documents, reviews, and activities, as tailored, must be performed.

Decomposition and integration:

- System increments are built, integrated, and tested separately, top down.

Incremental development for system components:

- Systems using Evolutionary Development Life Cycle are usually built in increments.
- Joint Requirements Planning (JRP) and Joint Applications Design (JAD) are employed for each increment. JRP and JAD groups should include technical and functional personnel,management personnel and members of the user community
- The increment is developed as a prototype.
- Looping through the phases occurs for each increment.

Concurrent development:

- Some components are built at the same time.
- Two or more system increments take place at the same time.

Testing:

- Testing begins early, with the first prototype demonstration.
- Stress testing is performed early - during Software Requirements Analysis.

Prototyping:

- Begins almost immediately
- Mini-life cycle with two levels:
  + Prototype development
  + Expansion of prototype to add levels of functionality.

Phases 1 through 6:

- Characteristics:
  + The system is built from the top level down.
  + System increments are handled separately through all the phases.

Phase 1: System Requirements Analysis & System Design:

- Update preliminary requirements.
- Describe the overall conceptual design of the system.
- Perform JRP to identify the system increment to be developed.
- Define the hardware platform.
- Describe the overall operating system functional requirements at a high level.
- Review the overall system design for compatibility.
- Procurement components (hardware, software, firmware) will exit the Evolutionary Development Life Cycle and re-enter later.
- Define interfaces.
- Determine major data categories.
- Produce the Software Development Plan:
  + Schedules and costs are less firm than with traditional life cycles.
  + Increase estimates by 10 + 20%.
  + Identify/define standards.
  + Develop the project schedule.
  + Define the project organization and responsibilities.
  + Define the Quality Assurance and Configuration Management Plans.
  + Address security issues.
  + Develop a preliminary prototyping concept and the overall approach to developing the evolving prototype into a completed system.
- Exit criteria:
  + Two documents
  + JRP sessions serve as reviews, and require concurrence.

Phase 2: Software Requirements Analysis:

- Rapid Analysis:
  + Preliminary Analysis:
    - JAD sessions are held.
    - An incomplete paper model is developed - presenting a high level view of functionality, major functions, and data.
    - The paper design is less extensive than with the traditional models.
  + Secondary Analysis:
    - The system functionality is discovered through prototyping.
    - Paper models expand.
- Initial Prototype Development:
  + This is the first attempt to develop a piece of the prototype.
  + It is performed each time a new level of functionality is added to the prototype.
  + The data base is prepared; the user interface and functional modules are developed.

- Prototype Iteration:
  + A working model is developed between users and developers.
  + Higher level system functions (components) are developed first.
  + Lower levels begin when higher levels are agreed upon.
  + Iteration stops when users completely agree with the prototype.
- External interfaces are described and documented.
- Specifications are updated as the system develops.
- The design includes all user interface requirements and other external interface requirements.
- Exit criteria:
  + Two documents
  + Updates to previous documents
  + JAD sessions serve as reviews
  + Software Requirements Review.
- Upon completion and concurrence by the customer:
  + The functional baseline is established (Software Requirements Specification (SRS))
  + Products are placed under configuration management.

Phase 3: Design:

- Preliminary Design:
  + Document the baselined prototype system architecture.
  + Stress test the prototype components (Computer Software Components (CSC) for performance.
  + Prove any design components with risk factors.
  + Begin design of the physical data base.
  + Design and document external interfaces.
  + Begin the Implementation Plan, with user involvement, and the Training Plan, using the Project Management Plan.
  + Expand the Test Plan and begin the Software Test Description Document (STDD).
  + Exit criteria:
    - Five documents
    - Updates of previous documents
    - Design Review.
- Detailed Design:
  + CSCs from the Preliminary Design are divided into CSUs.
  + Detailed specifications are produced for their coding.
  + The physical data base is finished.
  + Test cases are defined.
  + Stress tests for performance requirements are done.
  + Exit criteria:
    - Two documents
    - Updates of previous documents
    - Critical Design Review (optional).
  + Upon completion and concurrence by the customer:
    - Coding and unit testing may begin.

Phase 4: Code and Test:

- Develop code for remaining CSUs, if any.
- Develop test procedures.
- Integrate and test Computer Software Units (CSU), CSCs, to reach the Computer Software Configuration Item (CSCI) level.
- Informal project reviews take place, especially for critical components.
- Make necessary changes to Software Design Document, modify code, and re-test.
- "Practice" test CSCI, including stress tests.
- Record all test results.
- Integrate procured hardware, software, firmware with developed software, if available.
- Exit criteria:
  + Completed code and tests for the system increment
  + Ongoing documents
  + Updated documents
  + Test Readiness Review.
- Upon completion and obtaining concurrence:
  + Code, listings, and documentation are placed under developmental configuration management.
  + The formal test baseline is established.
  + The system increment is ready for acceptance testing.

Phase 5: System Acceptance Testing:

- Concurrent development efforts meet and merge.
- Integrate procured hardware, software, firmware with developed software into user's operational environment.
- Support the user in developing test plans, cases, and procedures for final test.
- Merge and test all subsystem components (CSCIs, Hardware Configuration Items (HWCIs).
- Test the system as a whole (all CIs as one CI).
- Record all test results.
- Make necessary changes to the prototype, either design or code; re-test and update documentation, through configuration management.
- Repeat all phases affected by changes.
- Support the customer's functional audit.
- Deliver the source code and documentation.
- Perform training.
- Exit criteria:
  + Five final documents
  + Updates of previous documents
  + Training completed
  + Formal Qualification Test Review.
- Upon completion and concurrence by the customer:
  + A product baseline is established.
  + The system increment is now fully operational.

+ The next system increment is developed by repeating the Evolutionary Development Life Cycle.

Phase 6: Implementation and Evaluation:

- Follow the Implementation and Training Plans.
- Set up a "production" configuration management control system.
- Move the fully tested system increment to operational status.
- If enhancing an existing system, merge the new system increment into the operational configuration of the existing system.
- The customer evaluates the installed system increment in the operational environment.
- Provide support to the customer to evaluate the system increment performance from both the business and technical standpoints.
- Make necessary changes to previous products and recycle through the Evolutionary Development Life Cycle model.
- Exit criteria:
  + Defined by the transition plan
  + Final meeting with the customer for concurrence .
- Upon meeting criteria:
  + The system increment is now in production.
  + The system increment has maintenance status.
- Deliver all documents.
- Perform training.

Key issues:

- Strong presence of user community throughout the cycle
- Careful integration of business change with information system design
- Commitment of top management to the concept
- Have Design Team in place before starting Software Requirements Analysis
- Attention to baselines, configuration management, critical milestones
- Validating critical components
- Completion of phases - must follow entrance and exit criteria
- Managing risk - reviews
- Availability of proper tools
- Staff experience with prototyping.

APPENDIX 2. STRUCTURED DEVELOPMENT LIFE CYCLE (SDLC) CHECKLIST

Phase 1: System Requirements Analysis and System Design

A. *System Requirements Analysis*

_____ 1. Define and document the purpose of the new system in the Preliminary System/Subsystem Specification (SSS).

_____ 2. Analyze and document the current system in the SSS.

_____ 3. Define and document new system objectives and requirements in the SSS.

_____ 4. Define and document system constraints or assumptions in the SSS.

_____ 5. Define and document major system functions in the SSS.

_____ 6. Define and document system performance characteristics in the SSS.

_____ 7. Define and document additional requirements, e.g., contingency, security in the SSS.

_____ 8. Produce a Preliminary SSS.

_____ 9. Perform and have the customer approve the System Requirements Review.

B. *System Design*

_____ 1. Allocate and document system requirements among hardware configuration items (HWCI), computer software configuration items (CSCI), and manual operations, in the System/Segment Design Document (SSDD).

_____ 2. Document allocation of requirements in the SSDD. Include major data sets, external interfaces, processing, and performance requirements.

_____ 3. Prepare a Preliminary Software (Hardware, Firmware) Requirements Specification (SRS) for each subsystem.

_____ 4. Define interfaces between system components and outside world.

_____ 5. Analyze interface components for complexity to determine the need for a separate Interface

Requirements Specification (IRS) document or configuration control.

_____ 6. Prepare a Preliminary IRS, as needed, for each interface.

_____ 7. Update the Preliminary SSS, as necessary.

_____ 8. Perform project planning and document it in the Software Development Plan (SDP):

- _____ a. Identify/define standards.
- _____ b. Develop a project schedule.
- _____ c. Define the project organization and responsibilities.
- _____ d. Define a Software Quality Assurance (SQA) Plan.
- _____ e. Define a Configuration Management (CM) Plan.
- _____ f. Identify security issues and procedures.

_____ 9. Perform and have the customer approve the System Design Review (SDR) to establish the functional baseline.

_____10. Place the approved SSS under CM control.

Phase 2: Software Requirements Analysis

_____ 1. Design and document user interfaces.

_____ 2. Design and document other interfaces.

_____ 3. Define, design, and document logical databases and files. Start the data dictionary.

_____ 4. Update the SRS to document all external designs.

_____ 5. Update the IRS(s) (if applicable) to document all external designs.

_____ 6. Update other previous products as necessary.

_____ 7. Perform and have the customer approve the Software Requirements Review to establish the allocated baseline.

Phase 3: Design - Preliminary Design

_____ 1. Allocate the subsystem (CSCI) software requirements to the next lower level (Computer Software Component (CSC).

_____ 2. Describe the interaction of the CSCs.

_____ 3. Describe the internal processing of each CSC. Define the general design for the internal structure of each of each CSC in the Preliminary System Design Document (SDD).

_____ 4. Begin the design of the physical data base(s).

_____ 5. Explore critical or risky design considerations (prototyping).

_____ 6. Identify, describe, and document common factors. Prove the design concepts as in #5.

_____ 7. Develop a general Software Test Plan (STP).

_____ 8. Design and document all external interfaces in Preliminary Interface Design Documents (IDD) as described as described in the IRS or SRS.

_____ 9. Begin development of the Implementation Plan, involving the user.

- _____ a. Schedule all implementation activities.
- _____ b. Develop specifications for staffing requirements.
- _____ c. Develop specifications for site preparation.
- _____ d. Develop specifications for communication requirements.
- _____ e. Identify support equipment purchases.
- _____ f. Develop specifications for the operational phase support needed.
- _____ g. Identify system document distribution.
- _____ h. Identify security requirements.

_____10. Begin development of the Training Plan, using the Implementation Plan and Project Management Plan (PMP).

_____11. Update any previous products, as needed.

_____12. Perform and have the customer approve the Preliminary Design Review

or

_____13. Return to previous phase(s) to revisit requirements, as necessary.

Phase 3: Design - *Detailed Design*

_____ 1. Put the physical database in final form and define the data dictionary to the lowest level.

_____ 2. Review CSCs in the Preliminary Design to determine the lowest level of program structure

Computer Software Units (CSUs).

_____ 3. Develop detailed programming specifications for each CSU (in the SDD and IDD).

_____ 4. Define test cases for all units (CSUs) and components (CSCs) of the design, in the Preliminary

_____ 5. Define CSCI test cases in the STD.

_____ 6. Start the Users Manual (SUM) and Computer System Operations Manual (CSOM).

_____ 7. Begin development of training material.

_____ 8. Update any previous products, as necessary.

_____ 9. Perform and have the customer approve the Critical Design Review.

_____10. Place the approved SDD under developmental configuration control.

Phase 4: Code and Test - *Code and Unit Test*

_____ 1. Assign CSU coding specifications to developers.

_____ 2. Develop and document CSU informal test procedures.

_____ 3. Perform CSU testing according to test procedures.

_____ 4. Document and file the results of tests.

_____ 5. Analyze any test problems and change design specifications (SDD), test procedures (STDD), or code, accordingly.

_____ 6. Re-test any changed code and document the results, following test procedures.

_____ 7. Place "passed" code under developmental software configuration control.

_____ 8. Place source code listings and any revised design specifications (SDD) under developmental documentation configuration control.

_____ 9. Develop, document, and file CSC test procedures.

Phase 4: Code and Test - *Integrate and Test*

_____ 1. Integrate CSUs to constitute a CSC.

_____ 2. Test the CSC according to test procedures.

_____ 3. Document and file the test results.

_____ 4. Analyze problems and change the design, test, code, and documentation accordingly.

_____ 5. Re-test any changed code according to test procedures.

_____ 6. Place "passed" CSCs under software developmental configuration control.

_____ 7. Place source listings and any revised design documents under documentation developmental configuration control.

_____ 8. Develop CSCI test procedures for each test case in the STDD and update the STDD.

_____ 9. Perform CSCI tests in preparation for formal testing.

_____10. Document and file the test results.

_____11. Revise the STDD, as appropriate.

_____12. Repeat any phase activities, as warranted by results of the test.

_____13. Update any previous products, as necessary.

_____14. Perform and have the customer approve the Test Readiness Review.

_____15. Place the approved software and documents under developmental configuration control establish a formal test baseline.

Phase 5: System Acceptance Test - *CSCI Testing*

_____ 1. Perform a formal qualification CSCI test for each CSCI according to the STDD.

_____ 2. Document the test results in a formal Software Test Report (STR) for each CSCI.

_____ 3. Modify the design or code as indicated by the results of tests. Re-test and update the STDD,

_____ 4. Prepare source code for each CSCI for delivery, as specified in the SRS.

_____ 5. Support the user in developing and documenting the final system test materials.

_____ 6. Complete operation and support documents (SUM, CSOM).

_____ 7. Baseline each successfully tested CSCI.

Phase 5: System Acceptance Test -*System Integration and Testing*

_____ 1. Integrate the system and perform a final systems test.

_____ 2. Support the user in reporting system integration test results (STR).

_____ 3. Modify the design, documents, or code, as indicated by the results of system integration tests. Re-test as required, using formal CM procedures.

_____ 4. Update the STDD, as necessary.

_____ 5. Prepare a formal Software Production Specification (SPS) for each CSCI.

_____ 6. Prepare and deliver a Version Description Document (VDD) for each CSCI.

_____ 7. Support the configuration audit performed by the customer.

_____ 8. Support the functional audit performed by the customer, as final acceptance testing.

_____ 9. Complete the Implementation Plan, Training Plan, and Training Materials.

_____10. Update any previous products, as necessary.

_____11. Perform and have the customer approve the Final Acceptance Review.

_____12. Place the products under Product Baseline control.

Phase 6: Implementation and Evaluation

_____ 1. Perform system installation according to the Implementation Plan.

- _____ a. Facility preparation and site checkout.
- _____ b. Hardware and software installation and checkout.
- _____ c. Operational phase-in.

_____ d. Operations support.
_____ e. Set-up of CM for maintenance support.

_____ 2. Perform training according to the Training Plan.

_____ 3. Deliver all documents to the customer as specified in the SDP.

_____ 4. Maintain other documents, as specified in the SDP, for at least 6-12 months following successful implementation.

_____ 5. Hold a final meeting with the customer when the evaluation period ends, to ensure customer

The system, now complete, enters production and maintenance status.

APPENDIX 3. LIMITED STRUCTURED DEVELOPMENT LIFE CYCLE (LDLC) CHECKLIST

Phase 1: System Requirements Analysis and Design

_____ 1. Define and document the purpose of the new system in the Preliminary System/Subsystem Specification (SSS).

_____ 2. Analyze and document the current system in the SSS.

_____ 3. Define and document new system objectives and requirements in the SSS.

_____ 4. Define and document system constraints or assumptions in the SSS.

_____ 5. Define and document major system functions in the SSS.

_____ 6. Define and document system performance characteristics in the SSS.

_____ 7. Define and document additional requirements, e.g., contingency, security in the SSS.

_____ 8. Document the functional description of the system and high-level system design in the SSS.

_____ 9. Perform project planning and document in the Software Development Plan (SDP).

- _____ a. Identify/define standards.
- _____ b. Develop a project schedule.
- _____ c. Define the project organization and responsibilities.
- _____ d. Define a Software Quality Assurance (SQA) Plan.
- _____ e. Define a Configuration Management (CM) Plan.
- _____ f. Identify security issues and procedures.

_____10. Submit the SSS and SDP to the customer for review and formal concurrence.

Phase 2: Software Requirements Analysis

If prototyping, start at step 1; otherwise, start at step 5.

_____ 1. Define and document the prototype concept in the Prototype Concept Document.

_____ 2. Develop the prototype with the user participating, including major interfaces.

_____ 3. Load data for the prototype as specified in the Prototype Concept Document.

_____ 4. Evaluate the prototype with the user/developer team, incrementally or one time. *Proceed to step 8.*

_____ 5. Design and document the user interfaces.

_____ 6. Design and document other interfaces.

_____ 7. Define, design, and document the logical database and files. Start the data dictionary if not already done.

_____ 8. Produce the SRS to document all external designs.

_____ 9. Update any previous products, as necessary.

_____ 10. Perform the Software Requirements Review and have the customer approve the external design of the subsystem, including interface requirements. This establishes the functional baseline.

_____ 11. Place the functional requirements in the Software Requirements Specification (SRS) under configuration control.

Phase 3: Design - *Preliminary Design*

_____ 1. Allocate subsystem Computer Software Configuration Item (CSCI) software requirements to the next lower level, the Computer Software Components (CSC).

_____ 2. Describe the interaction of CSCs.

_____ 3. Describe the internal processing of each CSC. Define the general design for the internal structure of each CSC in the Preliminary System Design Document (SDD).

_____ 4. Refine further the logical database and data dictionary to incorporate CSC preliminary design specifications.

_____ 5. Begin the design of the physical data base(s).

_____ 6. Explore critical or risky design considerations (prototyping).

_____ 7. Identify, describe, and document common factors. Prove design concepts as in step 5.

_____ 8. Develop a general Software Test Plan (STP).

_____ 9. Design and document all external interfaces in the Preliminary Software Design Document (SDD) as described in the SRS.

_____10. Begin development of the Implementation Plan, involving the user.

- _____ a. Schedule all implementation activities.
- _____ b. Develop specifications for staffing requirements.
- _____ c. Develop specifications for site preparation.
- _____ d. Develop specifications for communication requirements.
- _____ e. Identify support equipment purchases.
- _____ f. Develop specifications for operational phase support needed.
- _____ g. Identify system document distribution.
- _____ h. Identify security requirements.

_____11. Begin development of the Training Plan, using the Implementation Plan and Project Management Plan (PMP).

_____12. Update any previous products, as needed.

_____13. Perform and have the customer approve the Preliminary Design Review

or

_____14. Return to previous phase(s) to revisit requirements, as necessary.

Phase 3: Design - *Detailed Design*

_____ 1. Put the physical database in final form and define the data dictionary to the lowest level.

_____ 2. Review CSCs in the Preliminary Design to determine the lowest level of program structure, Computer Software Units (CSU).

_____ 3. Develop detailed programming specifications for each CSU (in the SDD).

_____ 4. Define test cases for all units (CSUs) and components (CSCs) of the design, in the Preliminary Software Test Description Document (STDD).

_____ 5. Define CSCI test cases in the STD.

_____ 6. Start the Users Manual (SUM).

_____ 7. Begin development of training material.

_____ 8. Update previous products, as necessary.

_____ 9. It is optional to perform and have the customer approve the Critical Design Review, but the customer must approve the SDD in preliminary form.

_____10. Place the SDD under developmental configuration control.

Phase 4: Code and Test - *Code and Unit Test*

_____ 1. Assign CSU coding specifications to developers.

_____ 2. Develop and document CSU informal test procedures.

_____ 3. Perform CSU testing according to test procedures.

_____ 4. Document and file the results of tests.

_____ 5. Analyze any test problems and change design specifications (SDD), test procedures (STD), or code, accordingly.

_____ 6. Re-test any changed code and document the results, following test procedures.

_____ 7. Place "passed" code under developmental software configuration control.

_____ 8. Place source code listings and any revised Design Specifications (SDD) under developmental documentation configuration control.

_____ 9. Develop, document, and file CSC test procedures.

Phase 4: Code and Test - *Integrate and Test*

_____ 1. Integrate CSUs to constitute a CSC.

_____ 2. Test the CSC according to procedures.

_____ 3. Document and file the test results.

_____ 4. Analyze problems and change the design, test, code, and documentation accordingly. Re-test according to procedures.

_____ 5. Place "passed" CSCs under software developmental configuration control.

_____ 6. Place source listings and any revised design documents under documentation developmental configuration control.

_____ 7. Develop CSCI test procedures for each test case in the STDD and update the STDD.

_____ 8. Perform the CSCI tests in preparation for formal testing.

_____ 9. Document and file the test results.

_____ 10. Revise the STD as appropriate.

_____ 11. Repeat any phase activities, as warranted by results of the test.

_____ 12. Update any previous products, as necessary.

_____ 13. Perform and have the customer approve the Test Readiness Review.

_____ 14. Place the approved software and documents under developmental configuration control to establish a formal test baseline.

Phase 5: System Acceptance Test - *CSCI Testing*

_____ 1. Perform a formal qualification CSCI test for each CSCI according to the STDD.

_____ 2. Document the test results in a formal Software Test Report (STR) for each system type test performed.

_____ 3. Modify the design, documentation, or code as indicated by the results of tests. Re-test and update the STDD, using formal CM procedures.

_____ 4. Prepare source code for delivery, as specified in the SRS.

_____ 5. Support the user in developing and documenting final system test materials.

_____ 6. Complete loading of database with "live" data.

_____ 7. Baseline each successfully tested CSCI.

Phase 5: System Acceptance Test - *Formal System Testing*

_____ 1. Integrate the system and perform a final systems acceptance test.

_____ 2. Support the user in reporting formal system test results (STR).

_____ 3. Modify the design, documents, or code, as indicated by the results of formal system tests. Re-test as required, using formal CM procedures.

_____ 4. Update the STD, as required.

_____ 5. Prepare a formal Software Production Specification (SPS) for the CSCI to support maintenance and formal review of final system configuration (serves as configuration audit).

_____ 6 Complete the Implementation Plan to include instructions on how to build software on the target machine (replaces Version Description Document).

_____ 7. Complete the Training Plan, and Training Materials.

_____ 8. Update any previous products, as necessary.

_____ 9. Perform and have the customer approve the Final Acceptance Review.

_____10. Place the products under Product Baseline control, ready to be implemented for operation and evaluation.

Phase 6: Implement and Evaluate

_____ 1. Perform system installation according to the Implementation Plan.

- _____ a. Facility preparation and site checkout
- _____ b. Hardware and software installation and checkout
- _____ c. Operational phase-in
- _____ d. Operations support
- _____ e. Set-up of CM for maintenance support.

_____ 2. Perform training according to the Training Plan.

_____ 3. Deliver all documents to the customer as specified in the SDP.

_____ 4. Maintain other documents, as specified in the SDP, for at least 6-12 months following successful implementation.

_____ 5. Hold a final meeting with the customer when the evaluation period ends, to ensure customer satisfaction.

The system, now complete, enters production and maintenance status.

APPENDIX 4. EVOLUTIONARY SYSTEM DEVELOPMENT LIFE CYCLE (EDLC) CHECKLIST

Phase 1: System Requirements Analysis and System Design the current system in the SSS.

_____ 1. Define and document the purpose of the new system in the Preliminary System/Subsystem Specification (SSS).

_____ 2. Analyze and document the current system in the SSS.

_____ 3. Define and document new system objectives and high level requirements in the SSS.

_____ 4. Define and document system constraints or assumptions in the SSS.

_____ 5. Perform Joint Requirements Planning (JRP) to identify and select the system increment to be developed and review the overall system design.

_____ 6. Define and document major system functional requirements at a very high level in the SSS.

_____ 7. Define and document system performance characteristics in the SSS.

_____ 8. Define and document additional requirements, e.g., contingency, security, in the SSS.

_____ 9. Include the high level system design in the SSS.

_____10. Perform project planning and document it in the Software Development Plan (SDP):

- _____ a. Identify/define standards.
- _____ b. Develop a project schedule.
- _____ c. Define the project organization and responsibilities.
- _____ d. Define a Software Quality Assurance (SQA) Plan.
- _____ e. Define a Configuration Management (CM) Plan.
- _____ f. Identify security issues and procedures.
- _____ g. Develop a preliminary prototype concept for planning.
- _____ h. Define the database load procedures.

_____11. Conduct JRP sessions to serve as a review of systems requirements analysis and design.

_____12. Obtain concurrence on the documents with the customer.

Phase 2: Software Requirements Analysis - *Rapid Analysis*

_____ 1. Preliminary Analysis - partial paper model of the system as a foundation to begin prototype development.

- _____ a. Conduct Joint Application Development (JAD) sessions to develop a high level view of the prototype functionality.
- _____ b. Identify the major essential functions and data related information.
- _____ c. Define a high level view of data requirements for the preliminary database schema.
- _____ d. Develop a preliminary architecture for the prototype control structure of the system event paths.

_____ 2. Secondary Analysis - expand the paper models and documentation as the prototype evolves with new discoveries.

_____ 3. Document the results of preliminary and secondary analysis in the preliminary Software Requirements Specification (SRS), which evolves with prototyping.

_____ 4. Design and document other interfaces, in the SRS.

Phase 2: Software Requirements Analysis - *Requirements Analysis*

Create the initial prototype based on the paper model.

_____ 1. Prepare the database and load live data or create test data.

_____ 2. Develop the user interface.

_____ 3. Develop functional modules, decomposing from high level to low level.

_____ 4. Update the SRS as necessary.

_____ 5. Repeat the process as necessary until the product is ready for the user to see.

Phase 2: Software Requirements Analysis - *Prototype Iteration*

Perform jointly with the customer during JAD sessions.

_____ 1. Demonstrate the initial prototype to the user, allowing the user the opportunity to exercise the system to satisfy functional requirements.

_____ 2. Document the desired changes from user feedback.

_____ 3. Modify the prototype, including the database and data dictionary.

_____ 4. Demonstrate the prototype again to the user to show the modifications.

_____ 5. Repeat the looping demonstration process until the user agrees that the prototype component is functionally correct.

_____ 6. Obtain formal approval of the prototype component.

_____ 7. Update the SRS to reflect changes in the prototype.

_____ 8. Add the next level of functionality to the prototype.

Phase 2: Software Requirements Analysis - *Completion of Phase*

_____ 1. Repeat the Rapid Analysis, Initial Prototype Development, and Prototype Iteration until the final prototype for this increment is developed and approved.

_____ 2. Prepare the final SRS, adding high level test criteria, if needed.

_____ 3. Start the Software Test Plan (STP).

_____ 4. Conduct a final, formal user review to approve the software requirements.

_____ 5. Evaluate the prototype against all criteria, with the design team of users and developer representatives, incrementally or as a one-time activity.

JAD sessions throughout the phase serve as a continuous review of user/software requirements.

_____ 6. Update any previous products, as necessary.

_____ 7. Perform and have the customer approve the Software Requirements Review to establish a

functional baseline.

_____ 8. Place the SRS and working model (prototype) under configuration control.

(Note: The Implementation Plan may be started here. See the Design Phase.)

Phase 3: Design - *Preliminary Design*

_____ 1. Document the system design as is:

- _____ a. Design the interaction of the Computer Software Components (CSC) of the prototype in the Software Design Document (SDD).
- _____ b. Define the internal processing of each CSC individually.
- _____ c. Define the general design of the internal structure of the CSC.
- _____ d. Document the design of the physical database(s).
- _____ e. Perform an informal review and walk through of design documents to ensure they reflect the system prototype.
- _____ f. Place the documents under configuration control to establish an informal, as is, prototype design baseline document.
- _____ g. Expand the Test Plan to include functional type testing, user acceptance testing, etc.
- _____ h. Begin the Software Test Description Document (STDD) to define requirements for performance stress testing, following the STP.

_____ 2. Stress testing:

- _____ a. Perform the stress test according to plans, to find performance problems. Document the results.
- _____ b. Analyze any problems to determine the solution.

_____ 3. Design and document any interfaces needing conventional code in a lower-level language.

_____ 4. Design and document external interfaces, following the SRS or solutions to stress testing.

_____ 5. Update the SDD for solutions to performance problems or external interfaces to be built.

_____ 6. Design tests to explore critical or risky design considerations (prototype the prototype).

_____ 7. Begin development of the Implementation Plan, involving the user:

- _____ a. Schedule all implementation activities.
- _____ b. Develop specifications for staffing requirements.
- _____ c. Develop specifications for site preparation.

_____ d. Develop specifications for communication requirements.
_____ e. Identify support equipment purchases.
_____ f. Develop specifications for the operational phase support needed.
_____ g. Identify system document distribution.
_____ h. Identify security requirements.

_____ 8. Begin development of the Training Plan, following the Implementation Plan and Project Management Plan (PMP).

_____ 9 Update any previous products, as needed.

_____ 10. Perform and have the customer approve the Preliminary Design Review

or

_____ 11. Return to previous phase(s) to revisit requirements, as necessary.

Phase 3: Design - *Detailed Design*

_____ 1. Put the physical database in final form to reflect new/modified design considerations and update the data dictionary.

_____ 2. Review CSCs in the Preliminary Design to determine the lowest level of program structure Computer Software Units (CSUs).

_____ 3. Develop detailed programming specifications for each CSU, in the SDD.

_____ 4 Define test cases for all units (CSUs) and components (CSCs) of the design, in the Preliminary Software Test Description Document (STDD).

_____ 5. Update the STDD for actual stress-test experience and functional type test cases.

_____ 6 Start the Software Users Manual (SUM).

_____ 7 Begin development of training material.

_____ 8. Update any previous products, as necessary.

_____ 9. Perform and have the customer approve the SDD. A Critical Design Review is optional.

_____ 10. Place the approved SDD under developmental configuration control.

Phase 4: Code and Test - *Code and Unit Test*

_____ 1. Assign CSU coding specifications to developers to produce code.

_____ 2. Develop and document CSU informal test procedures.

_____ 3. Perform CSU testing according to test procedures.

_____ 4. Document and file the results of tests.

_____ 5. Analyze any test problems and update design specifications (SDD), test procedures (STDD), or code, accordingly.

_____ 6. If there are changes to the prototype, return to Phase 2, Software Requirements Analysis, for iterations of prototype modification and demonstrations, updating of all documents, etc.

_____ 7. Re-test any changed code and document the results, following test procedures.

_____ 8. Place "passed" code under developmental software configuration control.

_____ 9. Place source code listings and any revised Design Specifications (SDD) under developmental documentation configuration control.

_____10. Develop, document, and file CSC test procedures.

Phase 4: Code and Test - *Integrate and Test*

_____ 1. Integrate CSUs into the working model (prototype) to constitute a CSC.

_____ 2. Test the CSC according to test procedures.

_____ 3. Document and file the test results.

_____ 4. Analyze problems and change the design, test, code, and documentation accordingly, following CM procedures.

_____ 5. Re-test any changed code according to test procedures, and document the results.

_____ 6. Place "passed" CSCs under developmental software configuration control.

_____ 7. Place source listings and any revised design documents under developmental documentation configuration control.

_____ 8. Develop Computer Software Configuration Item (CSCI) test procedures for each functional test case in the STDD and update the STDD.

_____ 9. Perform CSCI stress and functional tests in preparation for formal testing, following test procedures.

_____10. Document and file the test results.

_____11. Revise the STDD, as appropriate.

_____12. Repeat any phase activities, as warranted by results of the tests.

_____13. Update any previous products, as necessary.

_____14. Perform and have the customer approve the Test Readiness Review.

_____15. Place the approved software and documents under developmental configuration control to establish a formal test baseline for the system increment.

Phase 5: System Acceptance Test - *CSCI Testing*

_____ 1. Perform a formal qualification CSCI test for each CSCI according to the STDD.

_____ 2. Document the test results in a formal Software Test Report (STR) for each CSCI.

_____ 3. Modify the prototype, design, or code as indicated by the results of tests. Re-test and update the STDD, using formal CM procedures.

_____ 4. Prepare software/source code for delivery, as specified in the SRS.

_____ 5. Support the user in developing and documenting the final system test materials.

_____ 6. Complete the loading of the database.

_____ 7. Complete the Operation and Support Document (SUM).

_____ 8. Place each successfully tested CSCI under configuration control.

Phase 5: System Acceptance Test -*Formal System Testing*

_____ 1. Integrate the system and have the customer perform a final systems acceptance test.

_____ 2. Document formal system test results in the STR.

_____ 3. Modify the prototype, design, documents, or code, as indicated by the results of system tests. Re-test as required, using formal CM procedures.

_____ 4. Update the STDD, as necessary.

_____ 5. Prepare a formal Software Production Specification (SPS) (serves as a configuration audit).

_____ 6. Complete the Implementation Plan [replaces the Version Description Document (VDD)], Training Plan, and Training Materials.

_____ 7. Update any previous products, as necessary.

_____ 8. Perform and have the customer approve the Final Acceptance Review of the system increment.

_____ 9. Place the products under Product Baseline control.

Phase 6: Implement and Evaluate

_____ 1. Perform system installation according to the Implementation Plan.

- _____ a. Facility preparation and site checkout.
- _____ b. Hardware and software installation and checkout.
- _____ c. Operational phase-in.
- _____ d. Operations support.
- _____ e. Set-up of CM for maintenance support.

_____ 2. Perform training according to the Training Plan.

_____ 3. Deliver all documents to the customer as specified in the SDP.

_____ 4. Maintain other documents, as specified in the SDP, for at least 6-12 months following successful implementation.

_____ 5. Hold a final meeting with the customer when the evaluation period ends, to ensure customer satisfaction.

The system increment is now complete and enters production and maintenance status. The next increment of the system, if applicable, is developed by repeating the EDLC.

APPENDIX 5. ASSESSING THE BUSINESS AND TECHNOLOGICAL CHANGES THAT IMPACT THE SYSTEM DEVELOPMENT PROJECT

This appendix is used to assess and evaluate the business and technological change factors to guide the selection of a system development life cycle.

Assessing the Business Change

On a scale of 1 through 10, with 1 as the lowest and 10 the highest, rate each business change factor.

1. Are the steps or operations that make up the business process largely observable (low) or are you primarily in the position of either developing them or piecing the puzzle together as you progress (high)?

2. Are you building a system intended to support an existing set of steps and/or procedures (low) or to create and/or change a set of steps and/or procedures (high)?

3. Are the steps and procedures that make up the business process well understood and stable (low), or just now coming into existence within the effected organizations and unstable (high)?

4. Does the system propose to integrate or cut across one or two functional areas (e.g., policy, planning, logistics) within the effected organizations(s) (low). Or three or more functional areas (high)?

5. Will the system have little or no impact on existing personnel and/or organizations in terms of reporting structure, responsibilities, performance measures, required skills, and position descriptions (low) or moderate (medium) to significant impact (high)?

6. Is there an example (i.e., business model) for this system elsewhere within the government (low-medium) or in a closely-related industry (e.g., airline carriers or manufacturers) or are you breaking new ground (high)?

7. Is the data/information involved freely and readily available throughout the organization (low) or is it centrally managed and/or controlled by a functional area or an organization that may be reluctant to share it (medium/high)?

8. When development involves a large-scale application with other high business change scores, is there general user commitment and enthusiasm toward the aims of the project (low/medium) or a lack of commitment and enthusiasm (high)?

9. Does this project have the support of a highly placed champion and/or a senior management decision maker in the user organization management (low) or little of this level of support (high)?

10. Will only the AF organizations involved in the development use the system (low) or will the system be used by other AF organizations, other FAA organizations, other government organizations, or contractors (high)?

11. When the system will be used by multiple organizations, does the system support the status quo in how the external elements interact with the developing organization, in how they conduct business, or in the functions, responsibilities, skills, reporting requirements, and/or performance measures associated with the current personnel (low) or does the system imply change in one or more of these areas (high)?

Assessing the Technological Change

On a scale of 1 through 10, with 1 as the lowest and 10 the highest, rate the technological change factor.

1. Have the developers who will more than likely work on the project ever developed a system like this before (low) or never (high)?

2. Is this type of system common within the FAA (low) or uncommon (high)?

3. Is the primary technology to achieve the system objectives fully developed, widely used, and timely (low) or is it new (high) or emerging (highest)?

4. Can you satisfy some requirements using existing code from libraries or existing systems (low) or must all source code be written anew (high)?

5. Are the people within your organization that are available to work on the project familiar with the hardware environment associated with this system (low) or unfamiliar (high)?

6. Are the people within your organization that are available to work on the project familiar with the software environment associated with this system (low) or unfamiliar (high)?

7. Are the people within your organization that are available to work on the project familiar with the communications environment associated with the system (low) or unfamiliar (high)?

8. Are the people within your organization that are available to work on the project familiar with the standards and protocols that govern development of the system (low) or unfamiliar (high)?

9. Do organizational elements that benefit from the system have ultimate control over required data for the system (low), or is control shared with another organizational element (medium), or is data beyond your control (high)?

10. Are the data interfaces few and primarily internal to the existing system and effected organizations (low)? Are there many internal and external data interfaces that are stable in their design and technical implementation (high)? Are there mostly external interfaces that are unstable (highest)?

11. Is the system data flow limited to a single physical building (low) or is it distributed throughout various sites within the same organization (medium) or does the data flow extend to various organizations within the agency (high) or does the data flow extend to various organizations within other agencies (highest)?

12. When this is an on-line system, are the requirements for access to update or add information reasonable and readily achievable in the target hardware/software environment (both in terms of geography and response time) (low), ambitious (medium), or for a real-time system (high)?

Evaluating the Change.

Calculate separately the average score for the degree of change to business and the average score for the degree of change to technology. See paragraph 9-8 when finished.

When the score is from 1 to 4, the change factor is low, either 5 or 6 is medium, and from 7 to 10, the factor is high.

Low and high change factors should align with the guidelines for life cycle selection. When a medium change factor results, select the life cycle that seems appropriate based on all factors involved. However, it is usually better to lean toward high when the score is medium.

APPENDIX 6. SOFTWARE QUALITY ASSURANCE

1. General.

The guidelines provided within this appendix apply to all contractors providing AF with software development support. Adapted (verbatum in some instances) from the Software Engineering Institute's (SEI) Capability Maturity Model with their permission, these guidelines represent the best thinking and experience the computer software industry has to offer on this subject.

All IRM system development contractors to AF should have a Software Quality Assurance (SQA) process to support all the software development projects. Its purpose is to ensure that development is on schedule and that the products delivered are according to AF management expectations. Performed well, it will provide the AF Program Manager of major systems with appropriate visibility into the process being used by the project and of the products being built.

Software quality assurance involves reviewing and auditing system products and activities to verify that they comply with the applicable procedures and standards along with providing the AF Program Manager and other appropriate managers (in AF and the contractor organization) with the results of these reviews and audits.

The software quality assurance group should work with the project during its early stages to establish plans, standards, and procedures that will add value to the project and satisfy the constraints of the project and FAA policy. The software quality assurance group should participate in establishing the plans, standards, and procedures to ensure that they fit the project's needs and they will be usable for performing reviews and audits throughout the development life cycle. As the group reviews project activities and audits work products throughout the life cycle, it should provide management (AF and contractor) with visibility as to whether the project is adhering to its established plans, standards, and procedures.

Compliance issues are addressed within the project first and resolved there if possible. For issues unresolved at the project level, the software quality assurance group shall escalate the issue to an appropriate level of management for resolution.

2. Goals.

Contractor management should support the following AF software quality assurance goals:

a. Plan all software quality assurance activities.

b. Verify objectively that all products and activities adhere to the applicable standards, procedures, and requirements.

c. Inform affected groups and individuals of software quality assurance activities and results.

d. Ensure that contractor senior management addresses noncompliance issues that are unresolved at the project level.

3. Key Commitments.

For each system development project, the contractor management should ensure that the:

a. Software quality assurance function is in place on all AF corporate system development projects.

b. Software quality assurance group has a reporting channel to senior management within the contractor's organization that is independent of the project manager and design engineering group.

Since software quality assurance requires independence, contractor management should determine the organizational structure that will support software quality assurance's activities in context of the strategic business goals and business environment. Independence should provide the individuals performing the software quality assurance role with the organizational freedom to be the eyes and ears of senior management on the project; protect the individuals performing the software quality assurance role from performance appraisal by the management of the project they are reviewing; and provide senior management with confidence that objective information on the process and products of the project is being reported.

c. Senior management periodically reviews the software quality assurance activities and results.

4. Software Quality Assurance Group.

Contractor management shall identify a software quality assurance group responsible for coordinating and implementing software quality assurance for the project. This group shall typically be composed of departments, managers, and individuals who have responsibility for a set of tasks or activities. Depending on the assigned tasks or activities, the size of the project, the organizational structure, and the organizational culture, this group can vary form several full-time individuals to one part-time person.

5. Adequate Resources and Funding.

Contractor management should ensure there are adequate software quality assurance resources and funding planned and available for each system development project. Specifically management should ensure that:

a. A manager is assigned specific software quality assurance responsibilities for the activities.

b. A senior manager who is knowledgeable in the software quality assurance role and has the authority to take appropriate oversight actions, is designated to receive and act on software noncompliance items.

c. Tools are available to support software quality assurance, e.g., workstations, database programs, spreadsheet programs, and auditing tools.

6. Software Quality Assurance Group Training.

Contractor management should ensure that members of the software quality assurance group are trained to perform their activities. Calculate the average score for the degree of change to business and the average score for the degree of change to technology.

When the score is from 1 to 4, the change factor is low, either 5 or 6 is medium, and from 7 to 10, the factor is high.

Low and high change factors should align with the guidelines for life cycle selection. When a medium change factor results, select the life cycle that seems appropriate based on all factors involved. However, it is usually better to lean toward high when the score is medium.

7. Orientation.

Contractor management should ensure that members of the system project receive orientation on the role, responsibilities, authority, and value of the software quality assurance group.

8. Activities.

Contractor management should ensure that the following software quality assurance activities are performed for each system development project.

a. A software quality assurance plan project according to a documented procedure.

b. The software quality group's activities are performed in accordance with the software quality plan.

c. The software quality assurance group participates in the preparation and review of the project's software development plan, standards, and procedures.

d. The software quality assurance group reviews the software engineering activities to verify compliance.

e. The software quality assurance group audits designated software work products to verify compliance.

f. The software quality assurance group periodically reports the results of its activities to the software engineering group.

g. Deviations identified in the software activities and software work products are documented and handled according to a documented procedure. Typically this procedure specifies that:

h. The software quality assurance group conducts periodic reviews of its activities and findings with AF personnel, as appropriate.

9. Measurement and Analysis.

Contractor management should ensure that measurements are made and used to determine the cost and schedule status of the software quality assurance activities. Examples of measurements include:

a. Completions of milestones for the software quality assurance activities compared to the plan.

b. Work completed, effort expended, and funds expended in the software quality assurance activities compared to the plan.

c. Numbers of project audits and activity reviews compared to the plan.

10. Verifying Implementation.

Contractor management should ensure that the following verification of software quality assurance activities are completed:

a. The software quality activities are reviewed with senior management on a periodic basis. The primary purpose of these reviews is to provide awareness of and insight into software process activities at an appropriate level of abstraction and in a timely manner. The time between reviews should meet the needs of the organization and may be lengthy as long as adequate mechanisms for exception reporting are available.

b. The software quality assurance activities are reviewed with the project manager on both a periodic and event-driven basis.

c. The software quality assurance group reviews and/or audits the activities and work products for software project tracking and oversight and reports the results.

APPENDIX 7. CONTRACT SYSTEM DEVELOPMENT

1. General.

The directives and guidelines in this appendix were adapted from the Software Engineering Institute. (SEI).

2. Contract Management.

The contractor shall manage AF system development efforts in accordance with the methodology specified in the contract between AF and the contractor.

3. Audits.

The .Program Manager of a major system establishes the rights of AF to audit the contractor's performance including:

a. The right to conduct software quality audits of the tasks specified in the contractor's Software Quality Program Plan.

b. The right to conduct configuration audits at the contractor's facility.

4. Baselines.

The contractor will use baselines as the major progress milestones. The Program Manager of a major system will use them to determine whether a particular development effort is on schedule. When rescheduling is required, baselines will be used to assess the impact on the remainder of the development and the project in general.

5. Principles that AF Will Apply to Contract Management.

The Program Manager of a major system will ensure the following actions occur:

a. The Program Manager will establish basic system objectives at the start. Objectives consist of performance, function, cost, etc.

b. The Program Manager will ensure that specific functional requirements that are known are stated. Poorly understood functions will be stated conceptually until more is known about them.

c. The contractor will produce a documented plan to establish and validate requirements against the objectives. This can include prototypes, reviews, surveys, etc. The plan states what must be done to know the requirements are met before completion of the system.

d. A joint requirements effort will be performed with AF and contractor personnel to define the system functions with sufficient precision to permit design to start. Even though the requirements document is baselined, AF will consider requirements complete only after the design and development work are done. Requirements are expected to continue to change until the development is complete and new baselines are then established. AF feedback will be continual throughout the development process.

e. The contractor will document the objectives of any prototype, model, or test clearly before it begins. The requirement or design decision being validated must be known before starting. It must be known up from how success is determined from failure.

f. The contractor will fully define the development process up front. This will include process milestones that ensure performance.

g. The contractor will track, audit, and software quality assure the process and its deliverables throughout the development process.

6. Software Contract Management.

Once there is a mutual understanding of requirements between users and developers, the Program Manager of a major system will focus on what is being done rather than how the product is being built.

a. Developing Software Requirements. Three parties should be involved in this process which should be negotiating and creative: users, contracting agency (when it applies), and the developers. Three situations can occur requiring different approaches:

(1) Experienced users and developers. When both users and developers are experienced regarding the business aspects of the application, a relatively straight forward process of producing and

documenting traditional requirement statements, estimates, and plans is expected to be sufficient.

(2) Inexperienced designers. When designers are inexperienced in the business aspects of the application, the use of prototypes is recommended before major development investments are made. There will first be a reasonably informed agreement between AF and the contractor on what is needed.

(3) Inexperienced users. When users have no detailed operational experience with the application being built, it is essential for the contractor to produce an operational prototype of the end user functions and conduct operational tests. The tests should be a planned and instrumented series of simulated operations.

b. Prototypes. When building entirely new systems, it is desirable that an operational prototype of the entire system be built first. Industry has proven that the prototype followed by a full development program is generally much less expensive and time consuming then the full program without the prototype. With only the mainline code that is core to each function being built, and the unusual paths ignored, it is substantially easier to develop than a full system and answers the question, does this system do what is needed? The system will be more likely to perform as desired and meet AF expectations when it is initially delivered.

c. Managing the Software Process. The contractor will develop a plan that demonstrates the actual characteristics needed (e.g., performance). This demonstration will occur during the design phase when timely corrections are possible.

d. Project Tracking Considerations. Once an agreed-upon development plan is in place, the contractor will track performance against it in the following manner:

(1) Items tracked will be a natural result of the development process.

(2) Tracking will be distinguished from reviewing. There must be clear evidence that a planned item is 100 percent complete.

(3) Items tracked will support the plan.

e. Technical Reviews. Technical reviews are important throughout the development process. The reviews will always focus on how well the job is being done. Initially, the most important reviews will involve the requirements and operational concept (performed to ensure the right work is being done), and the development plan (to ensure it is being done correctly).

f. Quantitative Process Tracking. The contractor shall allocate the percent each development phase is of the total effort based on labor months involved and assign a value to each activity in the phase based on its fraction of the total job. Each checkpoint achieved must be for 100 percent completion of the activity with no credit for partial completion. Other quantitative tracking can consist of:

(1) Code size.

(2) Planned resources.

(3) Planned schedule.

(4) Number of modules completed (weighted by size).

(5) Tests successfully completed.

g. Quality Tracking. The specific quality indicators will be determined by the contractor's quality plan. The existence of the plan results in more care at every step during the process. Historically, when code is tested early, code quality improves earlier in the process reducing total test time.

APPENDIX 8. ACRONYMS AND GLOSSARY

ACRONYMS

ADP	Automated Data Processing
AF	Airways Facilities
AIS	Automated Information Systems
AISSO	Automated Information Systems Security Officer
AIT	Office of Information Technology
BPI	Business Process Improvement
CAEG	Computer Aided Engineering Graphics
CASE	Computer-Assisted Software Engineering
CIP	Capital Investment Plan
CM	Configuration Management
COTS	Commercial Off-The-Shelf
DBMS	Data Base Management System
DIRMM	Departmental (DOT) Information Resources Management Manual
DOT	Department of Transportation
DRR	Deployment Readiness Review
EDI	Electronic Date Interchange
ERC	AF Executive Resource Committee
FAA	Federal Aviation Administration
FIP	Federal Information Processing
FIRMR	Federal Information Resources Management Regulation
GAO	General Accounting Office
GNMP	General Network Management Protocol
GOSIP	Government Open Systems Interconnection Profile
GSA	General Services Administration
GWA	General Working Agreements
HQ	Headquarters
HW	Hardware
HW/SW	Hardware/Software
ICWG	Interface Control Working Group
ILS	Integrated Logistics Support
IM	Information Management
I/O	Input/Output

IRDS	Information Resource Dictionary System
IRM	Information Resources Management/Information Resources Manager
IRMC	Information Resources Management Committee
ISD	Information Systems Development
IT	Information Technology
KDP	Key Decision Point
LAN	Local-Area Network
NAS	National Airspace System
NASMAP	NAS Management Automation Program
NDI	Non-developmental Items
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NIST	National Institute of Standards and Technology
OA	Office Automation
OATS	Office Automation Technology and Services
OCC	Operations Control Center
OMB	Office of Management and Budget
OPR	Office of Primary Responsibility
OSE	Open Systems Environment
OSI	Open Systems Interconnection
OT&E	Operational Testing and Evaluation
POSIX	Portable Operating System Interface for Computer Environments
PRA	Paperwork Reduction Act
RAD	Rapid Application Development
RE&D	Research, Engineering and Development
RTP	Resource Tracking Progam
SMO	Senior Management Official
TIMS	Telecommunications Information Management System
TQM	Total Quality Management
WAN	Wide-Area Network

GLOSSARY

Configuration

The functional and/or physical characteristics of an information system (hardware/software) as set forth in technical documentation and achieved in a product.

Configuration Identification

The current approved or conditionally approved technical documentation for a configuration item as set forth in specifications, drawings, associated lists, and referenced documents.

Configuration Item

An aggregation of hardware/software/firmware, or any of its discrete portions, which satisfies an end-use function and is designated by the Government for configuration management.

Data Model

The data model provides a logical view of the data from the perspective of the information user, as opposed to the physical structure of electronically stored data. It reflects the information entities and relationships as employed by the enterprise.

Engineering Change Proposal

The request for an engineering change to an established configuration baseline and the documentation that supports the change request.

Federal Information Processing (FIP) Resources

FIP resources includes automatic data processing equipment as defined in Public Law 99-55 (40 U.S.C. 759(a)(2)), e.g. any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information by a Federal agency or under contract to a Federal agency. In addition to equipment, FIP resources include software, services, support services, maintenance, related supplies, and systems (an organized combination of FIP resources).

Firmware

Firmware is the computer software resident in hardware read-only-memory (ROM) devices, which cannot be readily modified under program control like other resident software.

Functional Plan/Strategic Plan

The Functional Plan or Strategic Plan is a major output of the Strategic Planning Process. It defines the mission, goals, and objectives of the organization, the gaps that must be addressed to realize the vision, and the strategies and associated actions that will be carried out by the organization.

Implementation Plan

The Implementation Plan defines how an organization will function, including organizational structure, resources, and operational procedures. It specifies how it will deliver services to customers and implement strategies designed to meet the requirements of the organization's mission.

Information Management

Information Management addresses the total set of requirements for the collection, integration, management, and dissemination of information needed day-to-day operations and decision-making processes of an organization.

Information Repository / Data Dictionary

The information repository maintains information on the rules and location of data contained in AF databases. It provides a means for maintaining consistent information on constraints and dependencies among data elements and objects used in AF information systems.

Information Resource Entity

An information resource entity or data element is the basic unit of data that can be identified or described.

Information Resource Management (IRM)

IRM has traditionally referred to the subset of Information Management that addresses administrative information and associated automated systems. As organizations have begun to address the business context of information, IRM has evolved to encompass a broader scope, including the acquisition, management, and distribution of all information that is required to meet the mission needs of the organization.

Information Technology (IT)

Information Technology refers to the specific systems and techniques that carry out Information Management functions, including hardware, software, and networking technologies, as well the methods and models that support planning and systems development.

Interoperability

Interoperability refers to the ability of FIP resources to provide services and data to and from other FIP resources regardless of specific proprietary associations of such resources.

Life Cycle

Life cycle in reference to system development refers to the complete span of time from the inception of the idea for an infomation system to the end of the system's useful life.

Major Information Systems

A major information system refers to one that is distinguished by its importance to an agency mission; its high life cycle cost; or its significant impact on the administration of FAA programs, finances, property, or other resources.

National Airspace System (NAS)

The facilities, equipment, regulations, procedures, and personnel which support the safe and efficient movement of all aircraft in U.S. airspace.

Office Automation Technology and Services (OATS)

The DOT OATS contract provides for standard user platforms, including hardware, software, and support services. For the FAA, the contract is managed by the Office of Information Technology (AIT).

Open Systems Environment (OSE)

The objective of the OSE is to ensure transportability of data and applications among information systems. The requirements for open systems are described in FIPS Pub 141, Government Open Systems Interconnection Profile.

Operations Control Center (OCC)

The concept of the Operations Control Center is a key component of the future vision of Airway Facilities operations. It is a centralized command-and-control facility for Airway Facilities systems with technology capable of remote maintenance monitoring, collection and analysis of performance data, coordination of maintenance activities, and compilation of all the information necessary for the life-cycle management of Airway Facilities equipment and facilities.

Proprietary

Proprietary means any item, usually commercial software of a specialized database, for which the Government or public does not have unlimited rights.

Public Domain Software

Public domain software refers for software products which have been released for general use and distribution.

Rapid Application Development (RAD)

Rapid Application Development is an approach to managing the system development process that aims to shorten development cycles through the use of prototypes and other techniques which match system capabilities to user requirements.

Real-time Data

Real-time data refers to information that is obtained and changes in a very short time relative to its access and display. Such information is distinguished from administrative data, which changes more slowly and which can be managed by traditional database management systems.

Records Management

Records Management refers to the management of media on whcih information is recorded and the control of the agency's program and administrative records.